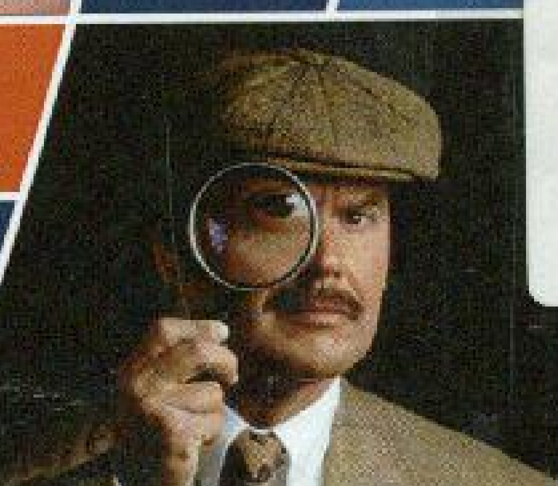
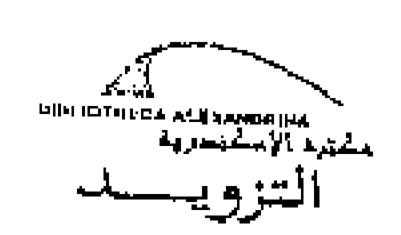
تكنولوجيا المعلومات
فى المجال الأمنى

د/ أشرف السعيد أحمد

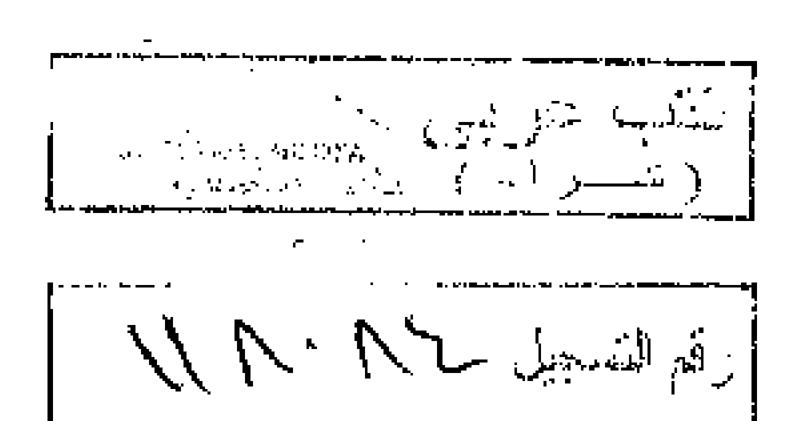


تكنولوجيا المعلومات فى المجال الأمنى



دكتور
أشرف السعيد أحمد

٢٠١٣



عنــوان الكتــاب: **تكنولوجيا المعلومات فى المجال الأمنى**

المــؤلــف: د. أشرف السعيد أحمد

الطبعة الأولــى: ٢٠١٣

رقــم الإيــداع: ٢٠١٢/٢٣٥١٢

الترقيم الــدولى: ٣ - ٠٢٩٠ - ٩٠ - ٩٧٧ - ٩٧٨



بسم الله الرحمن الرحيم

﴿قُلْ هَلْ يَسْتَوِي الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لَا يَعْلَمُونَ إِنَّمَا يَتَذَكَّرُ أُولُو الْأَلْبَابِ﴾

(سورة الزمر، آية ٩)

صدق الله العظيم



إهداء ..

إلى والدي حفظه الله.

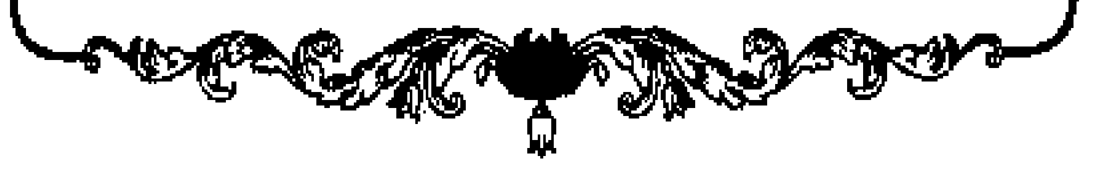
إلى روح أمي الطاهرة.

إلى شريكة عمري.

إلى بناتي العزيزات.

إلى حفيدي الغالي.

د. أشرف السعيد أحمد





تقديم:

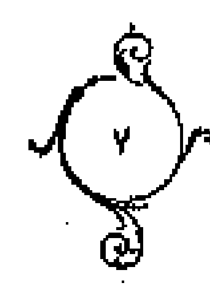
تُشكل المعلومات دورًا حيويًا فى حياة الأفراد والمجتمعات، فهي عنصر لا غنى عنه في أي نشاط نمارسه، فهى المادة الخام للبحوث العلمية، والمحك الرئيس لاتخاذ القرارات الصحيحة، وأضحى للمعلومة دورٌ مهم وحيوى فى نتاج البشر وتدبير الأمور، وتسهم فى التنمية وتنعكس على الإنتاج، وتشكل السلوك القويم بما ينعكس على التقدم الإيجابى للفرد والجماعة والدولة.

فقد كان لوزارة الداخلية الحرص على مواكبة التقدم التكنولوجى وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، لدعم مقومات الأمن والاستقرار اللازم لتحقيق التنمية الشاملة، والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية فى مجال تكنولوجيا المعلومات الأمنية لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية فى مصر، وذلك من خلال توفير البيانات والمعلومات الدقيقة اللازمة لتأمين مُتطلبات المجتمع، ومواكبة التطور السريع والمذهل فى تكنولوجيا الحاسبات الآلية والتطوير المستمر لآليات العمل الأمنى بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية المتقدمة وتوفير المعلومات والبيانات القادرة على التعامل مع مُتغيرات الأحداث، ولقد أثر التطور السريع لتكنولوجيا المعلومات تأثيرًا كبيرًا وبالغًا فى واقع العمل الأمنى.

وسنتناول فى هذا المؤلَّف موضوع تكنولوجيا المعلومات فى المجال الأمنى من خلال خمسة فصول:

الفصل الأول بعنوان: تكنولوجيا المعلومات، وسنتناول من خلاله ماهية التكنولوجيا وخصائصها، ومفهوم المعلومات، ومفهوم تكنولوجيا المعلومات، وأنواع نظم المعلومات.

الفصل الثانى بعنوان: تكنولوجيا المعلومات الأمنية، وسنتناول من خلاله نشأة



نظام المعلومات فى وزارة الداخلية، والتخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية، ومقومات بناء تكنولوجيا المعلومات الأمنية، وأهداف تكنولوجيا المعلومات الأمنية، وخصائص ومميزات المعلومات الأمنية، ومعايير جودة المعلومات الأمنية، تكنولوجيا المعلومات وصنع القرار الأمنى، ومدى الحاجة لتكنولوجيا المعلومات فى العمل الأمنى.

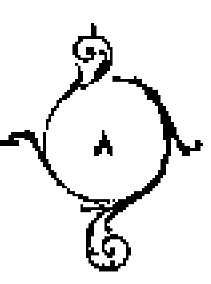
الفصل الثالث بعنوان: استراتيجية أمن المعلومات، وسنتناول من خلاله مفهوم أمن المعلومات، ومفهوم الاستراتيجية، ومحل الحماية، والمخاطر المحتملة، وأهم أساليب تأمين قواعد البيانات.

الفصل الرابع بعنوان: تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية، وسنتناول من خلاله مفهوم الحكومة الإلكترونية، تطبيقات وزارة الداخلية المصرية فى مجال الحكومة الإلكترونية، وتكنولوجيا المعلومات الأمنية فى مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية.

الفصل الخامس بعنوان: دور التقنيات الحديثة فى تطوير تكنولوجيا المعلومات الأمنية، وسنتناول من خلاله مفهوم التقنية البيومترية، وبصمة الإصبع، البصمة الوراثية.

وندعو الله أن نكون قد وفقنا فى المساهمة ولو بشكل بسيط فى عرض المعلومات الأساسية، التى تساعد الباحثين والمهتمين بمجال تكنولوجيا المعلومات الأمنية لمواكبة عصر تكنولوجيا المعلومات.

المؤلف





الفصل الأول

تكنولوجيا المعلومات

الفصل الأول
تكنولوجيا المعلومات

تمهيد:

إن فيض المعلومات الذى يواجه الأمم والشعوب أصبح النبض والعصب لجهود التنمية والتحديث؛ حيث يغطى كل مجالات الحياة المعاصرة من عملية واقتصادية واجتماعية وتعليمية وثقافية ودينية، وأضحى للمعلومة دور مهم وحيوى فى نتاج البشر وتدبير الأمور، وأصبح يقاس بمدى التقدم فى أية مهنة أو دولة أو منظمة أو فرد بما يتوافر لدى كل منهم من مستودع لا يتناقص من معلومات، وتشكل ذاكرة حية للمعارف والخبرات، وتسهم فى التنمية وتنعكس على الإنتاج، وتشكل السلوك القويم بما ينعكس على التقدم الإيجابى للفرد والجماعة والدولة. فالمعلومات تتطور بمعدلات سريعة بما يجعلها فى حالة تشكيل وتعديل على الدوام، وتكنولوجيا المعلومات تعمل على تحسين كفاءة المنظمات وفاعليتها.

وفى ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتى:

أولاً: ماهية التكنولوجيا وخصائصها.

ثانيًا: مفهوم المعلومات.

ثالثًا: مفهوم تكنولوجيا المعلومات.

رابعًا: أنواع نظم المعلومات.

أولاً- ماهية التكنولوجيا وخصائصها :

يعتبر لفظ التكنولوجيا من أكثر المفاهيم المتداولة للاستخدام فى الوقت المعاصر، من قِبل الفرد العادى والمتخصص، فهو مفهوم متعدد الجوانب والأبعاد ولا يوجد اتفاق بين المفكرين على تعريف واحد لها، ولكنه لا يخرج عن الإطار الذى يرى أنها مجرد تتويج للعقل البشرى الذى يسعى للسيطرة على الطبيعة وفق ما يخدم مصالحه، فهى نوع من المعرفة التي من الممكن اكتسابها ونقلها وتطويرها وتطبيقها بواسطة أفراد مؤهلين ومنتظمين فى هيئات وكيانات ومؤسسات مختلفة.

كلمة تكنولوجيا (Technology) هى كلمة يونانية تتكون من شقين الأول(Techno) ويعنى فن الصناعة أو التشغيل، والثانى (Logo) ويعنى علم أو منهج أى أن كلمة تكنولوجى فى معناها اللغوى تعنى «العلم التطبيقى للنواحى الصناعية»، هناك من يرى أن « التكنولوجيا ببساطة هى أسلوب أداء ويتضمن هيكلها مزيجًا مركبًا متفاعلاً من تجهيزات آلية، وعمالة، وطرق عمل تؤلِّف بين التجهيزات والعمالة فى إجراءات أداء بأسلوب محدد لإنتاج أو تقديم سلعة أو خدمة أو أكثر»[1]. ورأى آخر يرى أنها بمثابة وعاء يجمع بين جانبى العلم والفن؛ حيث يتمثل جانب العلم فى الاعتماد على نتائج الأبحاث العلمية فى التطبيقات التكنولوجية بينما يتمثل جانب الفن فى قدرة الإنسان على التحكم فى تلك التطبيقات ووضع مجموعة القيم التى تضمن استخدام تلك التكنولوجيا بما يحقق خدمة المجتمع بصورة جيدة. وهناك من عرَّفها بأنها«عبارة عن أشياء مادية، تشمل المنتجات والأدوات والأجهزة المستخدمة فى الإنتاج – الأنشطة أو العمليات – وهى تشمل طرق وأساليب الإنتاج، والمعرفة اللازمة لتطوير واستعمال المعدات والأدوات والأساليب للحصول على مخرجات محددة». ورأى آخر يرى أنها

(١) أحمد سيد مصطفى : إدارة الإنتاج والعمليات فى الصناعة والخدمات، مكتبة الأنجلو المصرية، الطبعة الثالثة، القاهرة، ١٩٩٧م ، ص٨٠.

«عملية تاريخية تعكس التفاعل بين الإنسان وإدراكه للبيئة»[1]. ويرجع السبب فى عدم تحديد مفهوم واحد للتكنولوجيا، إلى اختلاف مستويات التحليل التى اعتمد عليها المفكرون فى دراستهم للعلاقة بين التكنولوجيا والتنظيم، فمنهم من اهتم بدراسة التكنولوجيا على مستوى المنظمة، وهناك من اهتم بدراسة التكنولوجيا على مستوى مجموعات العمل داخل المنظمة وهناك فريق ثالث اهتم بدراسة التكنولوجيا على مستوى الأفراد[2].

والتكنولوجيا هى نوع من المعرفة التى من الممكن اكتسابها ونقلها وتطويرها وتطبيقها، وتنطوى على درجة كبيرة وعالية من التخصص، مما يسهل عملية اكتسابها أو تطبيقها، فهى ليست مجرد الأداة أو الوسيلة التى يستخدمها الإنسان فى حل مشاكله والتحكم فى بيئته، بل إنها تتسع لتشمل الظروف الاجتماعية التى أفرزت هذه الأداة، وكذلك الجوانب المختلفة للسلوك الاجتماعى فيما يخص تطبيقاته.

والتكنولوجيا هى عنصر ذو ثلاثة أبعاد:

١- البُعد الفنى وهو متمثل فى العلم والمعرفة المتاحة.

٢- البُعد التنظيمى والمتمثل فى توفير كافة احتياجات المجتمع من سلع وخدمات كما تساعد الإنسان على التغلب على المشاكل والصعوبات التى تواجهه.

٣- البُعد التطبيقى والمتمثل فى قدرة الإنسان على الاستفادة من المعرفة المتاحة، وهى تتسم بالديناميكية والتطور المستمر، وتلعب دورًا أساسيًا فى تحقيق التنمية الشاملة للمجتمع.

(1) Horrington Jon: Organization Structure And Information Technology, New York Prentice Hall International, 1991,P31.

(2) Yadav,D.S : Foundations Of Information Technology-3 rd ed, New age international limted publishers ,2006,P204.



خصائص التكنولوجيا:

١- التكنولوجيا علم مستقل له أصوله وأهدافه ونظرياته، ولا يتم فصل لفظ التكنولوجيا عن العلم، فلا يتصور أن تكون هناك تكنولوجيا إن لم تُرافق مع ثورة علمية[١].

٢- التكنولوجيا علم تطبيقي يسعى لتطبيق المعرفة.

٣- التكنولوجيا عملية تمس حياة الأفراد، وتعكس حضارة الشعوب، كما أنها الذاكرة الحية لهذا الشعب في زمن معين، والتطور البشري مرتبط بتطور التكنولوجيا.

٤- التكنولوجيا عملية شاملة لجميع العمليات الخاصة بالتصميم والتطوير، وهي تعنى بخطوات الحصول على الخدمة من المنظمات العامة، وتدفق العمل الذي يتم من خلال إعداد المستندات والملفات إلكترونيًا داخل المنظمة، والهدف الرئيسي لتحسين الإجراءات إلكترونيًا هو تقليل وإزالة فاقد العمليات وتبسيط العمل وتوفير تغذية مرتدة من العملية، وخفض فترة العمل وتقليل الأخطاء في أداء الخدمة[٢].

٥- التكنولوجيا هادفة، تهدف للوصول إلى حل المشكلات.

٦- التكنولوجيا متطورة ذاتيًا، وتتسم بالمرونة المستمرة في عمليات المراجعة ومدى قابليتها للتعديل والتجديد والتطوير فيها.

(1) Oliver. E.C. Chapman, R.J. French, C.S: Data processing And Information Technology -8 ed, DP Publications, Reviser, 1990, P154.

(2) Lucas, Henry C : Information Technology For Management -7 th ed (Boston :Irwin / McGraw -Hill, 2000) P122.

ثانيًا- مفهوم المعلومات :

المعلومات هى ناتج لتشغيل البيانات، وهى التى تعطى للبيانات معنى، وهى تزودنا بالأسس التى تقوم عليها القرارات[1]. وهى تجميع بيانات خام وتنظيمها بواسطة التصنيف والمقارنة وتفسيرها وتقديمها للاستخدام بعد التفهم العميق؛ حيث يؤدى ذلك إلى بزوغ المعرفة.

وهناك علاقة وثيقة بين المعلومات والمعرفة، فالمعلومات تزيد رصيد الإنسان من المعرفة، وإذا لم تقم المعلومات بهذه المهمة فلا توصف بأنها معلومات، والمعرفة حصيلة أو رصيد خبرات ومعلومات وتجارب ودراسة طويلة يملكها شخص معين مادى أو معنوى، وهى تختلف من شخص إلى آخر باختلاف المعلومات التى حصل عليها والتجارب التى خاضها والبيئة التى يعيش فيها، كما تختلف بالنسبة للفرد من وقت إلى آخر طبقًا لتلك الحصيلة والتي -غالبًا- تزداد مع الزمن[2].

مصادر المعلومات :

يتميز الإنسان بفضيلة العقل التى حباه الله إياها والتى تميزه عن كل المخلوقات، ومن ثَمَّ فإن المعلومات هى أداة الوصول إلى المعارف والمخترعات فى كافة المجالات لتطوير الحياة، ويتم جمع المعلومات لتوافر المعرفة لمواجهة المتطلبات الحالية أو المستقبلية، ذلك يمثل الدافع لجمع المعلومات، فهى لا تجمع بهدف جمع المعلومات، ولكن لتحقيق أهداف شخصية لمن قام بجمعها أو لتحقيق أهداف المنظمة، ومهما تنوعت وتعددت المعلومات فإنه يمكن الحصول عليها من مصادر داخلية أو مصادر خارجية[3].

---

(1) K. Samuelson and H. Borko and G.X.Aney : Information System And Network Amsterdam : North Holand Publishing Co.,1977).P47.

(2) Williams, Brian K, Sawyer, Stacey C : Using Information Technology,4 th ed,Boston: McGraw -Hill,2001,p127.

(3) Lucas, Henry C : Information Technology ,op.cit,p135.

أ- المصادر الداخلية:

هى المعلومات التى يحصل عليها الفرد أو تتجمع لدى المنظمة نتيجة للتصرفات والتفاعلات الداخلية فى المنظمة، وهى تتجمع لدى الفرد أو المنظمة من خلال الأرشيف الخاص بالمنظمة، أو نظام المعلومات بالمنظمة الذى يتضمن المكاتبات والسجلات والتقارير والملفات والنشرات والدوريات ... إلخ، التى تصدرها إحدى الإدارات الشرطية، أو المعلومات الشفوية التى تتم من خلال قنوات الاتصال المختلفة، والمعلومات التى يتم الحصول عليها من التحريات أو من المتواجدين فى محل الحادث.

ب- المصادر الخارجية:

هى المعلومات التي تتعلق بالمتغيرات الاقتصادية والسياسية والثقافية، والمصادر الخارجية تشمل المعلومات التى تأتى من مصادر خارج الفرد أو المنظمة، ولكنها ذات صلة أو تأثير على الفرد أو المنظمة مثل بيانات أو معلومات من النقابات المهنية أو الحالة السياسية أو الاجتماعية أو الأمنية أو بيانات عن منظمات مماثلة أو الإحصاءات التى تصدرها الجهات المختلفة[1].

وتتمثل أنواع مصادر المعلومات فيما يأتى:

١- مصادر المعلومات العملية:

وهى المعلومات التى تتعلق بأنشطة الفرد أو المنظمة العملية المختلفة، وذلك من خلال القنوات الرسمية الخاصة بالمنظمة وغير الرسمية، وتشمل جميع المعلومات التى تتعلق بهذا النشاط أو ذات الصلة به.

---

(١) محمد محمد الهادى: التطورات الحديثة لنظم المعلومات المبنية على الكمبيوتر، القاهرة، دار الشروق، ١٩٩٣م، ص٧١.

٢- المصادر العلمية:

وهى تتعلق بالمعلومات العلمية والتكنولوجية المتصلة بمجال نشاط الفرد أو المنظمة، ويمكن الحصول عليها من قاعدة البيانات الخاصة بالمنظمة أو المنظمات المتخصصة فى تلك المجالات العلمية والتكنولوجية والفنية المتخصصة، كأكاديمية البحث العلمى والتكنولوجى ومراكز ومعاهد البحوث العلمية والفنية[١].

٣- المصادر الثقافية:

وهى المعلومات التى يحصل عليها الفرد أو المنظمة من وسائل الإعلام وأجهزة الثقافة، مثل الإذاعة، والتليفزيون وأبحاث المنظمات الثقافية المتنوعة والمكتبات العامة وما تصدره الدولة من نشرات.

٤- المصادر الذاتية:

هى مجموع المعلومات التى يختزنها الإنسان فى ذاكرته وما اكتسبه من خبرات ومعارف، من خلال التعليم وتعامله وتجاربه واختزنها فى ذاكرته[٢] .

الشروط التى يجب مراعاتها عند جمع المعلومات:

إن جمع المعلومات ليس عملية مرسلة، وإنما يجب أن تحكمها قواعد حتى لا تفقد قيمتها وتنفق الجهود فى سبيل الحصول على معلومات أقل أهمية أو تؤدى إلى تجميع أكبر قدر من المعلومات، مما يقلل من كفاءة النظام لذلك كان من الضرورى التعرض لبعض القواعد التى تعمل على توفير المعلومات الضرورية والأساسية لتحقيق أهداف

(١) عصمت عبد الله الشيخ : دور نظم وتكنولوجيا المعلومات فى تيسير وفاعلية العمل الإدارى، دار النهضة العربية، ١٩٩٨، ص٤٥.

(٢) طارق إبراهيم الدسوقى : الأمن المعلوماتى «النظام القانونى لحماية المعلوماتى»، القاهرة، دار الجامعة الجديدة للنشر، ٢٠٠٩، ص٣٧.

النظام عند جمع المعلومات من مصادر خارجية ومنها:

١ - الارتباط بالموضوع أو نشاط المنظمة:

أن تكون هذه المعلومات مرتبطة بالموضوع الذى سيتم جمع المعلومات من أجله وأن تكون متصلة اتصالاً مباشرًا بأنشطة وأهداف المنظمة ومؤثرة على هذا النشاط، وأن يتحاشى جمع معلومات هامشية أو ثانوية، بل يجب التركيز على المعلومات الأساسية الضرورية لتحقيق الهدف أو التأثير ذاته على مجالات الأنشطة المختلفة.

٢ - أن تكون المعلومات حديثة:

يراعى أن تكون المعلومات التى يقوم بجمعها الفرد أو المنظمة تمثل أحدث المعلومات فى مجال النشاط إلا فى حالة الأبحاث أو التقارير التى توضح التطور التاريخى للظاهرة أو الحدث.

٣ - الثقة فى مصادر المعلومات:

يراعى أن تكون المصادر التى تجمع المعلومات موضع ثقة من الناحية العلمية أو البحثية، وأن تكون مصادرها محددة ودقيقة، حتى تكون ذات قيمة. بالإضافة إلى ذلك فإن المعلومات قد تكون متوفرة فى أكثر من مصدر أو فى أكثر من موقع بالنسبة للمصدر الواحد؛ حيث إن كثرة المصادر ووفرتها وتعدد الأماكن بالنسبة للمصدر الواحد قد تجعل من المستحيل تغطيتها كلها، ومتابعة التطورات والتحديث فى كل منها، وفى هذه الحالة يجب وضع أولويات بالنسبة لهذه المصادر، وتعدد الأماكن بالنسبة للمصدر الواحد[1]، وأن يكون أساس المفاضلة هو التعمق وحداثة المعلومات بالإضافة إلى مدى شمول المعلومات وتغطيتها لنوع المجال أو النشاط، أو مجال البحث، ويستلزم

(1) Yadav,D.S, op. cit, p215.

وجود المعلومات توفر وعاء يحتويها وهو ما يطلق عليه بالوثيقة أو بمصدر المعلومات بأشكالها وأحجامها المختلفة، وللمعلومات أبعاد أهمها[1]:

١- **الكمية**: والتي تقاس بعدد الوثائق، الصفحات، الكلمات، الرسوم، والصور.

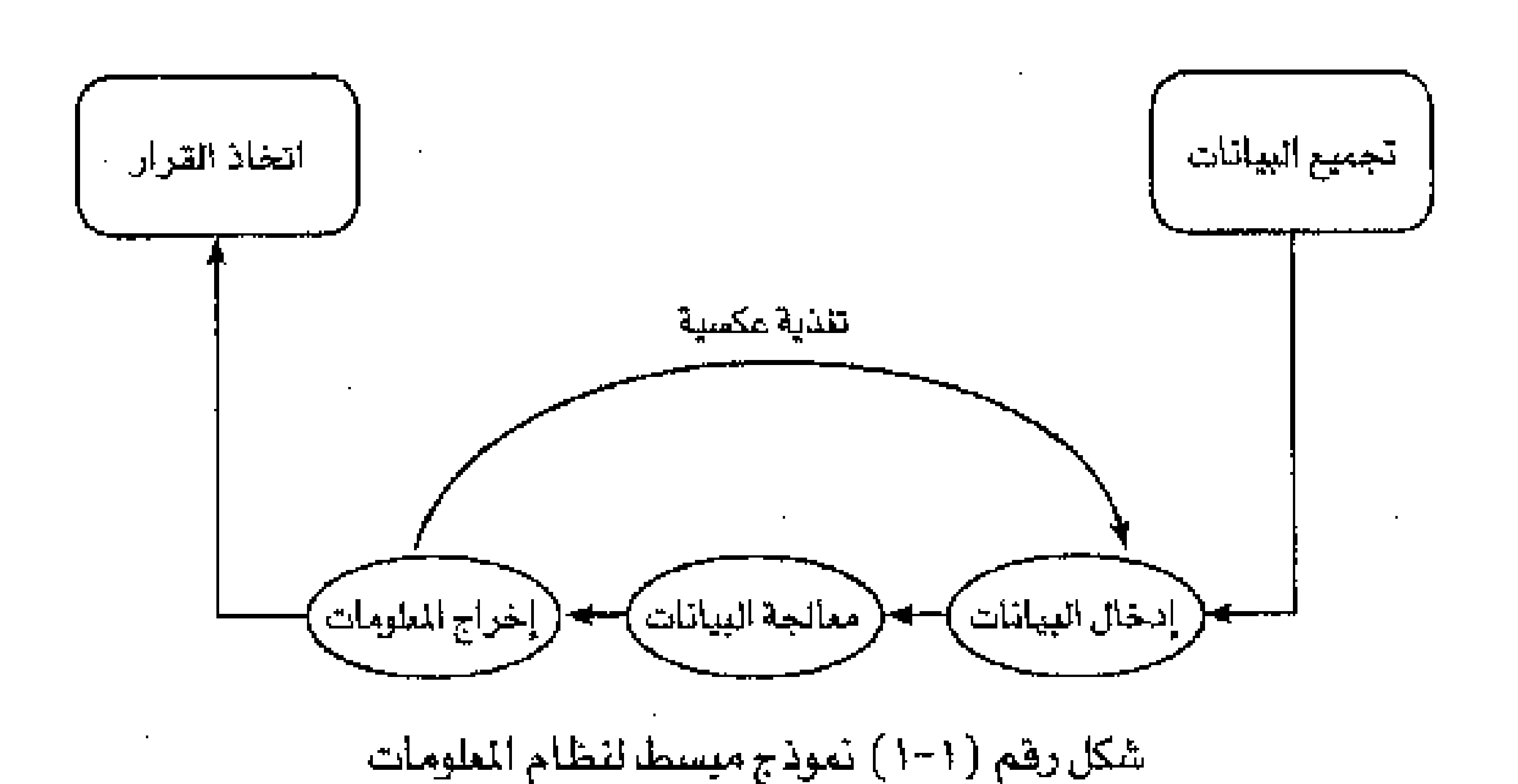
٢- **المحتويات**: وهي معنى المعلومات.

٣- **البنية**: وهي تشكل المعلومات والعلاقة المنطقية بين نصوصها وعناصرها.

٤- **اللغة**: وهي الرموز والحروف والأرقام التي يعبر بواسطتها عن الأفكار.

٥- **الجودة**: وهي أن تكون المعلومات كاملة وصحيحة وذات فائدة.

٦- **العمر**: وهو الفترة الزمنية التي تكون فيها المعلومات ذات قيمة.



شكل رقم (١-١) نموذج مبسط لنظام المعلومات

(1) Weisman, H.M : **Information Systems Services And Centers**, London: John Wiley, 1972, p13.

ثالثًا- مفهوم تكنولوجيا المعلومات :

يعتبر مفهوم تكنولوجيا المعلومات من أكثر المفاهيم استخدامًا فى الدراسات المعاصرة فهو مفهوم متعدد الجوانب والأبعاد، وهى أحدث مفرزات التطور التكنولوجى، وأدى التطور التكنولوجى المتمثل فى الاتصالات إلى إلغاء الحواجز بين الدول، ولقد تباينت اتجاهات الباحثين فى دراستهم لتكنولوجيا المعلومات، فهناك من اهتم بالمتغيرات والأبعاد الفنية وعرف تكنولوجيا المعلومات باعتبارها أدوات وتطبيقات هندسية تقوم بتنفيذ ما تتلقاه من أوامر وتعليمات(1)، مع إبراز دور التكنولوجيا فى الحصول على المعلومات؛ حيث عرَّف البعض تكنولوجيا المعلومات «أنها تشمل جميع أشكال التكنولوجيا التى تمكّن الأفراد من خلق ومعالجة المعلومات».

ونرى أن هذا التعريف خلط بين مفهومى البيانات والمعلومات؛ حيث تستخدم التكنولوجيا فى معالجة البيانات، والتى تعتبر بمثابة المادة الخام، للحصول على المعلومات، التى تمثل المنتج النهائى.

وهذا ما دفع البعض إلى تعريف تكنولوجيا المعلومات بأنها «تطبيق للتكنولوجيا الإلكترونية ومنها الحاسب الآلى والأقمار الصناعية وغيرها من التكنولوجيات المتقدمة لإنتاج المعلومات التناظرية والرقمية وتخزينها واسترجاعها وتوزيعها ونقلها من مكان إلى آخر»(2). وتتميز التعريفات السابقة بأنها أوضحت أن معالجة المعلومات تتم بشكل إلكترونى أو باستخدام التكنولوجيات الإلكترونية.

وهناك من يرى أن تكنولوجيا المعلومات «هى مزيج من تكنولوجيا الاتصالات

---

(1) Gershenfeld, Neil: The Physics Of Information Technology, Cambridge; New York : Cambridge University Press ,2000 ,p95.

(٢) حسن عماد مكاوى : **تكنولوجيا الاتصال الحديثة فى عصر المعلومات**، الطبعة الأولى، القاهرة، الدار المصرية اللبنانية، ١٩٩٣، ص٧١.



وتكنولوجيا الحاسبات الإلكترونية وقد أصبحت تكنولوجيا المعلومات الآن هى الزاد الرئيسى للتطوير التكنولوجى»[1]، وهناك من يُعرِّف تكنولوجيا المعلومات «بأنها حصيلة تزاوج وتفاعل ثلاث تكنولوجيات متمثلة فى، تكنولوجيا الحاسبات؛ وذلك بما تقدمه من حواسب فائقة القدرة وتجهيزات متنوعة تيسر للإنسان إمكانية التحاور معها، تكنولوجيا البرمجيات؛ والتى تشمل نظم تصميم وتنفيذ وإدارة قواعد البيانات ونظم استخدام الحاسبات فى التطبيقات المختلفة ونظم التخطيط وتنفيذ واختيار البرمجيات بمساعدة الحاسب، وأخيرًا تكنولوجيا الاتصالات؛ بما تقدمه من أساليب وتقنيات تساعد على ربط الحاسبات ونظم المعلومات بعضها ببعض فى أنظمة متكاملة على كافة المستويات» ونرى أن هذا الرأى يركز على إبراز الأنواع التكنولوجية المختلفة التى ساهمت فى ظهور وانتشار تكنولوجيا المعلومات، ولم يهتم بالأهداف التى تسعى هذه التكنولوجيا إلى تحقيقها أو الأنشطة التى يتم من خلالها تحقيق تلك الأهداف؛ حيث يرى أن تكنولوجيا المعلومات هى مزيج بين ثلاث تكنولوجيات متمثلة فى تكنولوجيا الحاسبات الرقمية، وتكنولوجيا تخزين البيانات وتكنولوجيا الإشارات الرقمية والاتصال عن بُعد[2]. وهناك من يرى أن مصطلح تكنولوجيا المعلومات «يشمل جميع أنواع التكنولوجيات المستخدمة فى جمع ومعالجة أو تبادل واستخدام المعلومات بأشكالها المختلفة».[3] وهو يركز على أجهزة الحاسبات والبرمجيات فقط؛ حيث يميل إلى استخدام الحاسبات الإلكترونية والبرمجيات لتحويل وتخزين، وحماية ومعالجة واسترجاع المعلومات من أى مكان وفى أى وقت، ونرى أن هذا التعريف يتسم بالعمومية الشديدة ومن الممكن أن ينطبق على أى

---

(١) أحمد سيد مصطفى : انعكاسات التكنولوجيا على العنصر البشرى فى المنظمات العربية، ورقة عمل نشرت بمجلة آفاق اقتصادية، العدد٧٣، مجلد ١٩، ١٩٨٩م، ص٩.

(٢) عماد عبد الوهاب الصباغ : علم المعلومات، دار الثقافة للنشر والتوزيع ، قطر، ٢٠٠٤م، ص ١٨٠.

(3) E.Wainright Martin et al : Managing Information Technology : What Managers Need To Know?,(New Jersey : Prentice Hall , 1999).p 24.



نظام لمعالجة البيانات بما في ذلك النظم اليدوية أو التقليدية التي تعتمد على الأدوات والأجهزة ذات الإمكانيات المحدودة، وهناك من نظر إلى تكنولوجيا المعلومات على أنها نظام فرعي، يهتم بأجهزة الحاسب الآلي وأجهزة الاتصالات.

وتتمثل تكنولوجيا المعلومات في استخدام أجهزة الحاسبات للبرمجيات والاتصالات في إدخال وتشغيل وتخزين ونقل المعلومات، وهي تعتبر نتاج تزاوج وتفاعل ثلاث تكنولوجيات من أجل تحقيق هدف معين وهو توفير الوقت وسهولة في التنفيذ من خلال الآتي:

١ - تكنولوجيا الحاسبات:

وذلك بما تقدمه من حواسب فائقة القدرة وتجهيزات متنوعة تيسر للإنسان إمكانية التحاور معها، والسرعة في تنفيذ الأوامر والعمليات الحسابية والمنطقية والإمكانيات الهائلة للحفظ والاسترجاع وإعداد التقارير والإحصائيات[1].

٢ - تكنولوجيا البرمجيات:

والتي تشتمل على نظم تصميم وتنفيذ وإدارة قواعد البيانات ونظم استخدام الحاسبات في التطبيقات المختلفة ونظم تخطيط وتنفيذ واختيار البرمجيات بمساعدة الحاسب.

٣ - تكنولوجيا الاتصالات:

وذلك بما تقدمه من أساليب وتقنيات تساعد على ربط الحاسبات ونظم المعلومات بعضها ببعض في أنظمة متكاملة على كافة المستويات، وسرعة نقل المعلومات والمشاركة في البيانات والأجهزة من خلال شبكات نقل المعلومات.

---

(١) علي عبد الهادي مسلم : مذكرات في نظم المعلومات المبنية على الكمبيوتر- المبادئ والتطبيقات، مركز التنمية الإدارية، جامعة الإسكندرية، ١٩٩٤م، ص١١٧.

ولقد أحدثت تكنولوجيا المعلومات تأثيرات جوهرية فى النظم الادارية من أهمها:

١- تحقيق الاستخدام الأمثل للموارد البشرية والفنية والمادية المتاحة للمنظمة والعمل على تنميتها كمًا وكيفًا.

٢- خلق قنوات اتصال جديدة من خلال شبكات الحاسبات والاتصالات سواء على مستوى المنظمة أو على المستوى القومي أو العالمي مما مكّن من زيادة سرعة تدفق ومعالجة وتبادل المعلومات وتطوير أساليب إدارية حديثة كالاجتماعات والتفاوض وعقد الصفقات عن بُعد.

٣- مساعدة المديرين على التخلص من أعباء المهام الروتينية مما أتاح لهم إمكانية استخدام فائض فى أوقاتهم للعمل فى مجال التخطيط الاستراتيجى ورسم السياسات ولقد انعكس ذلك بشكل واضح فى رفع كفاءة الإدارة العليا[1].

٤- ساهمت فى زيادة قدرة النظم الإدارية على التكيف السريع مع بيئة العمل الإدارى، من خلال توفير وسائل اقتصادية فعّالة لتخزين واسترجاع ومعالجة البيانات، وتقديمها إلى متخذ القرار فى الوقت المناسب[2].

تعتبر تطبيقات تكنولوجيا المعلومات أكثر انتشارًا فى المجالات الإدارية بالمقارنة مع المجالات الأخرى، فهى تؤثر مباشرة فى نظم الاتصال واتخاذ القرارات.

---

(1) Lucas, Henry C, op. cit, p105.

(2) Fletcher, Keith : Marketing Management And Information Technology, New York: Prentice Hall, 1995,p42.



رابعًا- أنواع نظم المعلومات :

هناك العديد من أنواع نظم المعلومات لتلبية الاختلافات في حاجة القيادات إلى المعلومات في الجهة أو المنظمة، وهي تشمل نظم المعلومات التشغيلية، النظم المعرفية، ونظم تجهيز المكاتب آليًا، ونظم المعلومات الإدارية، ونظم دعم القرارات، ونظم دعم الإدارة العليا، والنظم الخبيرة[١].

١- نظم تشغيل البيانات :

يهدف هذا النوع من نظم المعلومات إلى خدمة المستويات التشغيلية داخل الجهة، ويعتمد على الحاسب الآلي لتسجيل البيانات الروتينية، وتتمتع نظم التشغيل بالآتي:

- رسم حدود المنظمة وبيئتها من خلال ربط جميع فروعها.
- تعد نظم المعلومات منتجة للمعلومات وإعدادها للاستخدام في الجهة أو إدارات أخرى.

٢- النظم المعرفية:

تهدف تلك النظم إلى دعم العاملين بالجهة في مجال المعرفة والمعلومات من خلال ضمان وصول المعرفة والمعلومات بشكل متكامل داخل الجهة. وهي تعني الإضافة العلمية والثقافية من مصدر أو أكثر؛ حيث تؤدي هذه النظم المعرفية إلى اتساع إدراك الإنسان فتجعله قادرًا على معالجة أية مشكلة تواجهه في مجالات المعرفة التي تعلمها[٢].

(1) O'Brien, James A : Management Information Systems, 3rd ed ,Chicago: Irwin, 1996, p119.

(٢) علاء عبد الرازق السالمي : نظم إدارة المعلومات، الدوحة، قطر، المنظمة العربية للتنمية الإدارية، ٢٠٠٢م، ص٢٢١.

٣- نظم تجهيز المكاتب آليًا:

تُعد تلك النظم نوعًا خاصًا من نظم تشغيل المعلومات والتي يمكن استخدامها في نطاق أعمال وأنشطة الإدارات والمكاتب، ويقصد بتجهيز المكاتب كل أنواع نظم الاتصالات الرسمية، وغير الرسمية، المتعلقة بتوصيل المعلومات المكتوبة، وغير المكتوبة من شخص إلى آخر سواء داخل الجهة أو خارجها، ومن أمثلة الأجهزة المستخدمة في تجهيز المكاتب البريد الإلكتروني، البريد الصوتي، شبكات الحاسب الآلي، اجتماعات الفيديو.

٤- نظم المعلومات الإدارية:

هي مجموعة من النظم الفرعية التي يؤدي تفاعلها إلى إنتاج المعلومات التي تغطي الاحتياجات المختلفة للأنشطة الإدارية، ويتزايد حجم المعلومات التي تتعامل من خلالها نظم معلومات الجهات أصبحت نظم معالجة البيانات غير قادرة على توفير احتياجات متخذ القرار من معلومات واتجهت إلى الاعتماد على نظم المعلومات المبنية على الحاسب الآلي.

٥- نظم دعم القرارات:

هي نظم معلومات تهدف إلى مساعدة المديرين والقيادات لاتخاذ قرارات غير متكررة، وتعتمد على نظم تشغيل المعلومات ونظم المعلومات الإدارية، ويتم تصميم نظم دعم القرارات استجابة للاحتياجات غير المخططة من المعلومات[١] .

٦- نظم دعم الإدارة العليا:

هي تلك النظم التي يتم تصميمها لمساندة القيادة العليا التي لها تأثير ملموس على سياسات وخطط واستراتيجيات الجهة أو المنظمة، وتتعامل تلك النظم مع القرارات

---

(١) أحمد سيد مصطفى: المدير العربي في عالم متغير، القاهرة، بدون ناشر، ص١٢٨.



التى تلعب البيئة الخارجية دورًا ملموسًا ومؤثرًا عند اتخاذها، وهى قرارات ذات درجة عالية من عدم التأكد.

٧- النظم الخبيرة:

تستخدم النظم الخبيرة لمساندة متخذ القرار فى التعامل مع القرارات غير الروتينية والتى لا يمكن التنبؤ بها، وتعتمد تلك النظم غير الروتينية على نتائج ما يسمى بالذكاء الاصطناعى؛ حيث تقوم تلك النظم على فكرة محاكاة عملية اتخاذ القرار التى يقوم بها المتخصص، وتتشكل العناصر الأساسية لبنية المعلومات من جزأين رئيسيين وهما:

أ- نظم الحاسبات الآلية:

هى تتضمن المكونات المادية والبرمجيات والبيانات والملفات والاتصال عن بُعد وهى تعد العنصر الرئيسى لتطبيقات النظم، وبالتالى فإن نجاح الجهة يتوقف على مقدرة تلك النظم على توفير الاحتياجات للجهة حاليًا ومستقبلاً[١].

ب- نظم التطبيقات الإدارية:

هى مجموعة من العمليات المنتظمة التى تمد المديرين بالمعلومات اللازمة لمساعدتهم فى تنفيذ الأعمال واتخاذ القرارات، وتشمل بيانات الموارد البشرية والمادية التى يتوقف على تحقيق أهدافها[٢].

(١) على فهمى: نظم دعم اتخاذ القرار والأنظمة الذكية، القاهرة، دار الكتب للنشر والتوزيع، القاهرة، ٢٠٠٤م، ص٧١.
(2) Lucas, Henry C, op. cit, p92.



الفصل الثانى

تكنولوجيا المعلومات الأمنية

الفصل الثاني
تكنولوجيا المعلومات الأمنية

تمهيد:

أصبحت فلسفة استخدام تكنولوجيات المعلومات الأمنية في مجالات الحياة المعاصرة علامة مُميزة وضرورة عصرية لا غنى عنها، وهدف استراتيجي في إطار السياسة الأمنية المُعاصرة، بُغية تدعيم القيم الإنسانية والأخلاقية، واحترام القانون وسيادة الشرعية الدستورية، وصيانة حقوق الإنسان، وترسيخ قواعد العدالة الجنائية، والارتقاء بمُستوى الخدمات الأمنية الجماهيرية، وباعتبارها النبض والعصب لجهود التنمية الاقتصادية، والاجتماعية، والثقافية، والعلمية.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي:

أولاً: نشأة نظام المعلومات في وزارة الداخلية.

ثانيًا: التخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية.

ثالثًا: مقومات بناء تكنولوجيا المعلومات الأمنية.

رابعًا: أهداف تكنولوجيا المعلومات الأمنية.

خامسًا: خصائص ومميزات المعلومات الأمنية.

سادسًا: معايير جودة المعلومات الأمنية.

سابعًا: تكنولوجيا المعلومات وصنع القرار الأمني.

ثامنًا: مدى الحاجة لتكنولوجيا المعلومات في العمل الأمني.

أولاً- نشأة نظام المعلومات فى وزارة الداخلية :

تعد وزارة الداخلية من أولى الوزارات التى تحرص على مواكبة التقدم التكنولوجى وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، لدعم مقومات الأمن والاستقرار اللازم لتحقيق التنمية الشاملة، من خلال توفير البيانات الحديثة والمعلومات الدقيقة اللازمة لتأمين مُتطلبات المجتمع، ومواكبة التطور السريع والمذهل فى تكنولوجيا الحاسبات الآلية من خلال التطوير المستمر لآليات العمل الأمنى بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية المتقدمة بتوفير المعلومات والبيانات القادرة على التعامل مع مُتغيرات الأحداث.

مركز الحاسبات الإلكترونية بوزارة الداخلية :

البداية كانت فى ١٥ مايو ١٩٧٦، عندما أعطى السيد/ ممدوح سالم رئيس الوزراء فى ذلك الوقت إشارة البدء لعمل أول نظام حاسب آلى (Main Frame) بمركز الحاسبات الإلكترونية بوزارة الداخلية، وهو ثانى حاسب آلى فى مصر ومنطقة الشرق الأوسط، وقد أُنشأ لخدمة أغراض مراقبة الحدود والتسجيل الجنائى، وشملت شبكة الاتصال بهذا الحاسب عدد ١٨٠ نهاية طرفية تعمل عن بُعد بخطوط مؤجرة (Leased Line) تربط مصلحة الجوازات وميناءى القاهرة الجوى والإسكندرية البحرى (بالنسبة لنظام مراقبة الحدود) ومديريات أمن القاهرة،الإسكندرية، أسيوط بالنسبة لنظام (التسجيل الجنائى)، بلغت السعة القصوى لذاكرة هذا الحاسب ٢٥٦ كيلو بايت والسعة التخزينية للأقراص الصلبة ٢٥ ميجا بايت، وقد استمر العمل بهذا النظام حتى عام ١٩٨٤م[1].

وكان هذا النظام يهدف إلى ما يلى :

- الكشف الفورى على المغادرين والقادمين عبر مطار القاهرة الجوى وميناء

(١) ندوة تكنولوجيا المعلومات الأمنية سنوات من التحديث والإنجاز، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠٠٤م، ص١٢.



الإسكندرية البحرى ومقارنة بياناتهم بقوائم الممنوعين بمصلحة وثائق السفر.

- تسجيل بيانات الأشخاص المطلوبين ومن لهم معلومات جنائية للاستفادة بهذه المعلومات فى حالات الاستعلام أو طلب معلومات لأغراض أعمال البحث والتحرى.

الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية :

فى عام ١٩٨١ صدور القرار الجمهورى رقم (٦٢٧) لسنة ١٩٨١م بإنشاء مراكز معلومات بأجهزة الدولة ، وتتبعه صدور القرار الوزارى رقم (٤٠٥) لسنة ١٩٨٢ بإنشاء الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية أكبر الأثر فى تطوير وميكنة نظم العمل بكافة جهات الوزارة، وخطت الوزارة خطوة مهمة فى هذا المجال؛ حيث شُكلت اللجنة العليا لنظم المعلومات بالقرار الوزارى رقم (٨٨١٥) لسنة ١٩٩٣والتى أوكل إليها مهمة وضع الاستراتيجية والخطط والبرامج المحددة الأهداف ووسائل تحقيقها والمدى الزمنى اللازم للتنفيذ والمحدد بدقة وذلك لعمل منظومة معلومات متكاملة للوزارة تقوم على عدة محاور وتشمل قواعد بيانات متكاملة على المستويين الجغرافى والنوعى فى مجالات مختلفة وتشمل، المعلومات الأمنية، المعلومات المالية، المعلومات الإدارية، العمليات (نظم القيادة والسيطرة)، الأنشطة الخدمية للمواطنين[1].

شبكة الإنترانت لوزارة الداخلية :

نظرًا للتطور المعلوماتى السريع كان لوزارة الداخلية السبق فى تطوير أسلوب العمل باستخدام تقنيات شبكات الحاسبات الآلية، والقرار بإنشاء شبكة معلومات وزارة الداخلية الموحدة الأثر الأكبر والفعَّال فى تعظيم الأداء الأمنى، وتطبيق منظومة الحكومة الإلكترونية.

(١) للمزيد راجع القرار الوزارى رقم (٤٠٥) لسنة ١٩٨٢بشأن إنشاء الإدارة العامة للمعلومات والتوثيق والهيكل التنظيمى لها، وطبيعة العمل ومهام كل إدارة فرعية وقسم بها.



بتاريخ ٢٥ يناير ٢٠٠١م أُعطيت إشارة البدء لعمل شبكة الإنترانت التى تتيح انسياب المعلومات وتبادلها بين قطاعات وأجهزة الوزارة بأسلوب تقنى متطور، وفى إطار من السرية وعدم القدرة على اختراقها من خارج الوزارة، بهدف رفع مستوى الأداء والتعامل بأسلوب عصرى مع معطيات القرن الحادى والعشرين وكيفية الاستفادة المثلى منها للعبور على المعوقات الزمنية والنمطية الروتينية ، وبما يتيح إمكانية اتخاذ القرار السليم المرتكز على قاعدة معلومات أمنية مؤمنة مدخلاتها ومخرجاتها[١].

ثانيًا- التخطيط الاستراتيجى لتطوير نظم المعلومات بوزارة الداخلية :

فى ظل الاعتماد على تكنولوجيا المعلومات كان لابد من وجود هدف استراتيجى تسعى الوزارة من أجل تحقيقه، من خلال تحقيق مجموعة أهداف أخرى فرعية، وتنفيذ مجموعة من الإجراءات لتحقيق الهدف الفرعى ومن أهم تلك الأهداف لتطوير نظم المعلومات بوزارة الداخلية تتمثل فيما يلى:

١- وضع خطة بعيدة المدى للمعلوماتية تتوافق مع خطة وزارة الداخلية الاستراتيجية وتلبى احتياجات الخطط الأمنية الأخرى.

٢- توفير المعلومات الأمنية المتكاملة على مستوى الجمهورية لكافة أجهزة البحث بمديريات الأمن والإدارات والمصالح والمنافذ وفروعها الجغرافية.

٣- ربط وتوحيد جميع أنظمة المعلومات بكافة جهات الوزارة بما يحقق تكامل نظم المعلومات الأمنية من خلال شبكة معلومات موحدة، مما يسهم فى سهولة وسرعة تبادل المعلومات فى إطار السرية وعدم القدرة على اختراقها، من خلال شبكة معلومات وزارة الداخلية.

---

(١) ندوة تكنولوجيا المعلومات الأمنية سنوات من التحديث والإنجاز، مرجع سابق، ص١٦.

٤- تطوير العمل بالأقسام والمراكز بإدخال أجهزة الحاسبات الآلية بها وربطها بقاعدة بيانات التسجيل الجنائى والمحكوم عليهم الهاربين من خلال شبكة معلومات وزارة الداخلية.

٥- تطوير العمل بأقسام الرقابة الجنائية واستحداث المنظومات الآلية للذكاء الاصطناعى ونظم الخبرة بما يسهم فى دراسة الظواهر الإجرامية وإصدار الإحصائيات والتقارير بما يعزز القدرة على العمل الجماعى ووضع خطط التأمين والضبط لتكون متوافقة مع المواقف الأمنية المختلفة.

٦- الاعتماد على نظم الخرائط الجغرافية والتى تسهم فى رصد البؤر الإجرامية والتفاصيل الطبوغرافية لمداخل ومخارج تلك البؤر.

٧- دعم الدوريات الأمنية والأكمنة الثابتة والمتحركة بأجهزة حاسبات مرتبطة بشبكة معلومات وزارة الداخلية لتحقيق الفحص الأمنى بمحل الاستيقاف.

٨- العمل على إتاحة أكبر قدر من خدمات وزارة الداخلية الجماهيرية عبر شبكة الإنترنت الدولية للتسهيل على المواطنين الحصول على الخدمة.

٩- وضع البرامج التدريبية ولتنمية الموارد البشرية من الضباط والأفراد والعاملين المدنيين فى مجال استخدام الحاسبات الآلية.

ثالثًا- مُقومات بناء تكنولوجيا المعلومات الأمنية:

واكبت مشروعات تكنولوجيا المعلومات الأمنية، أحدث ما توصلت إليه الثورة العلمية والتكنولوجية، من أجل خدمة أهداف التنمية، من خلال الآتى:

- بناء شبكة معلومات مُتطورة طبقًا لأحدث التقنيات الحديثة فى وسائل الاتصال، لتطوير أساليب العمل والتشغيل بمُختلف أجهزة الوزارة .



- بناء نُظم معلومات تُحقق التكامل بين أجهزة الوزارة على المُستوى (النوعي - الجغرافي)، وتكفل مُعالجة المشاكل والمواقف الأمنية وإدارة الأزمات.
- بناء قواعد بيانات لكافة مجالات العمل بالوزارة (الأمنية - الخدمية - التعليمية - التدريبية - الإدارية - المالية).
- الاهتمام بإعداد كوادر مُدرَّبة لرفع مُستوى الأداء الشُرطي وتدريس علوم نُظم المعلومات بجميع الكليات والمعاهد الشُرطية لجميع ضباط وأفراد الشرطة والعاملين المدنيين بالوزارة.

البنية الأساسية لشبكة الإنترانت لوزارة الداخلية:

تعد الإنترانت شبكة معلومات مبنية بتكنولوجيا الإنترنت ممتدة جغرافيًا إلى كافة قطاعات الوزارة ومديريات الأمن والإدارات العامة والمصالح والمنافذ الحدودية وأقسام ومراكز الشرطة بجمهورية مصر العربية، وقوامها حاسبات رئيسية ذات سعات تخزين ضخمة بالمركز الرئيسي وحاسبات خادمة بجهات الوزارة محمل عليها مواقع (Web Sites) تلك الجهات، وقد تم ربط الحاسبات الخادمة بالحاسبات الرئيسية عبر شبكة اتصالات رقمية مستخدمة خطوط البنية التحتية للشبكة القومية للاتصالات، كما تم وضع مجموعة من القيود التأمينية للشبكة لغلقها تمامًا لكافة الجهات والأفراد ويصرح فقط للجهات الشرطية بالدخول على مواقع الشبكة.

مكونات شبكة الإنترانت :

تتكون شبكة معلومات الوزارة (الإنترانت) من ثلاثة أجزاء رئيسية، هي :

١ - شبكة الاتصالات (Communication) :

في بداية نشأة شبكة الإنترانت تم الاعتماد في بناء شبكة الاتصالات على البنية الأساسية

التحتية للشبكة القومية للاتصالات باستخدام خطوط (PRI) للمركز الرئيسى واستخدام خطوط الاتصال (UP DIAL) للمستخدمين بخواص (ISDN) لسرعات تصل ما بين ٦٤ كيلو بايت إلى ١٢٨ كيلو بايت، كما استخدمت الخطوط المؤجرة (LEASER LINE) فى بعض القطاعات والمديريات للدخول إلى المركز الرئيسي، وتصل الطاقة الاستيعابية لعدد المستخدمين لشبكة الإنترانت إلى ٥٠٠ مستخدم لحظيًا، أما الآن يتم الاعتماد على الشبكة الاستراتيجية لوزارة الداخلية بالإضافة إلى شبكة (الواى ماكس).

٢- الحاسبات الآلية (Web Server) :

يتم استخدام الحاسبات الآلية كما يلى :

أ- حاسبات الويب الرئيسية (MAIN WEB SERVER) :

تحتوى حاسبات الويب على البوابة الرئيسية لشبكة معلومات وزارة الداخلية (MAIN PORTAL)، ويمكن من خلال البوابة الرئيسية الدخول إلى كافة مواقع جهات الوزارة سواء المحملة على الحاسبات الخادمة بالمركز الرئيسى أو المحملة على الحاسبات الخادمة بجهات الوزارة.

ب- حاسبات قواعد البيانات (DATABASE SERVER):

تتمتع حاسبات قواعد البيانات بإمكانية تخزين عالية مع استخدام تكنولوجيا (CLUSTER) فى تخزين وتداول البيانات.

جـ- حاسبات تأمين الاتصالات (REMOTE ACCESS SERVER) :

شبكة الإنترانت هى شبكة معلومات مغلقة وغير مصرح لأية جهة غير أمنية الدخول إلى مواقعها، وقد تم استخدام حاسبات تأمين الدخول تعمل على قنوات اتصال (PRI) لاختيار رقم طالب الخدمة، ويصرح فقط للأرقام المسموح لها بالدخول لتصفح مواقع الشبكة.

د- حواسب التأمين (FIRE WALL) :

روعى فى إنشاء شبكة المعلومات اتخاذ كافة التدابير الأمنية فى تداول ونقل البيانات باستخدام تكنولوجيا التشفير وحاسبات الحائط النارى (FIRE WALL) كما استخدم نظم التامين (ISA FIRE WALL) لتأمين الدخول على التطبيقات بالشبكة.

٣- نظم إدارة شبكات الاتصال :

تم دعم شبكة المعلومات بنظم تشغيل الإدارة الشبكات عن بُعد للوقوف على مشاكل التشغيل سواء لخطوط أو أجهزة الاتصال أو الحاسبات الخادمة والحاسبات العميلة، مع توافر إمكانية التداخل عن بُعد لمعالجة كافة مشاكل الشبكة.

مقومات شبكة الإنترانت :

تتعدد خدمات البوابة الرئيسية لشبكة معلومات وزارة على الإنترانت، وقد تم تصنيفها إلى ثلاثة محاور رئيسية هى:

- **المحور الأول - إعلامى :**

يهدف إلى إعلام الضباط والعاملين بالوزارة بتوجيهات القيادات العليا والقرارات الوزارية والكتب الدورية وأهم الأحداث الأمنية الجارية، وأوجه الرعاية الاجتماعية والصحية التى تقدمها الوزارة.

- **المحور الثانى - الاستعلام :**

يهدف المحور الثانى إلى إجراء الاستعلامات المطلوبة من خلال التطبيقات الأمنية بالشبكة، ويمكن من خلال الشبكة فحص المشتبه فيهم من خلال قاعدة بيانات مصلحة الأمن العام، والاستعلام عن السوابق والاتهامات أو بيانات المحكوم عليهم الهاربين، كما تتيح تطبيقات الغياب والمفقودين من التعرف على الجثث المجهولة، وكذا

الاستعلام عن السيارات التى يتم ضبطها والتعرف على السيارات المبلغ بسرقتها، كما يمكن الاستعلام عن الكتب الدورية والقرارات الوزارية والقوانين التى تخدم معظم مجالات العمل وغير ذلك من الخدمات الصحية والاجتماعية التى تقدمها الوزارة.

• **المحور الثالث - تبادل البيانات :**

تم توفير خدمة البريد الإلكترونى عبر شبكة الإنترانت، وقد تم تنفيذ تطبيق البريد الإلكترونى اعتمادًا على الكوادر الفنية المتخصصة من ضباط الوزارة لتحقيق خصوصية الاستخدام وسهولة التعامل مع أدوات التطبيق باللغة العربية لتبادل رسائل بين كافة جهات الوزارة فى إطار من السرية والسرعة وتداول المكاتبات بهدف تحقيق شعار «حكومة بلا أوراق».

رابعًا - أهداف تكنولوجيا المعلومات الأمنية :

استخدام تكنولوجيات المعلومات الأمنية فى مجالات الحياة المُعاصرة أصبحت علامة مُميزة وضرورة عصرية لا غنى عنها، وهدف استراتيجى فى إطار السياسة الأمنية المُعاصرة، بُغية تدعيم القيم الإنسانية والأخلاقية، واحترام القانون وسيادة الشرعية الدستورية، وصيانة حقوق الإنسان، وترسيخ قواعد العدالة الجنائية، والارتقاء بمُستوى الخدمات الأمنية الجماهيرية، وباعتبارها النبض والعصب لجهود التنمية الاقتصادية، والاجتماعية، والثقافية، والعلمية.

وانطلاقًا من هذا المفهوم، قامت وزارة الداخلية المصرية بتنفيذ عددًا من المشروعات المعلوماتية، بدءًا من مشروعات الميكنة والتطوير التى كان متعارف عليها من قبل، ووصولاً إلى مشروعات التنمية المعلوماتية والحكومة الإلكترونية، التى تُمثل قمة التحديث الحالى، بُغية تحقيق الأهداف الآتية :

- مواكبة التطور السريع والمُذهل فى تكنولوجيا الحاسبات الآلية، من خلال



التطوير المُستمر لآليات العمل الأمني، بما يضمن الارتقاء بمُستوى أداء الأجهزة الشُرطية.

- الارتقاء بمُستوى الأداء للعاملين، من خلال وجود الأدوات المعلوماتية والأنظمة الاتصالية، مما يخلق لديهم الحوافز الشخصية للابتكارات والمهارات، ويختصر الوقت والجهد ويُحسّن الأداء.
- سرعة الاستجابة للمواقف الأمنية، بتوفير المعلومات والبيانات القادرة على التعامل مع مُتغيرات الأحداث على الأصعدة القومية والإقليمية والدولية.
- دعم مقومات الأمن والاستقرار اللازم لمسيرة العمل الوطني، وتشجيع الاستثمار الوطني والأجنبي، وتحقيق التنمية الشاملة، من خلال توفير البيانات الحديثة والمعلومات الدقيقة اللازمة لتأمين مُتطلبات المُجتمع.
- العلاقة بين الشُرطة والشعب وتوثيق أوجه التعاون بينهما، باستخدام التقنيات المعلوماتية المُتقدمة وتقديم خدمات أمنية أفضل وأيسر للمواطنين، والعمل على تبسيط وتيسير إجراءات حصولهم على الخدمات الشُرطية.

خامسًا - خصائص ومميزاتها المعلومات الأمنية :

للمعلومات أهمية في حياتنا الحاضرة فيتم الاعتماد عليها في جميع المجالات المختلفة، وبقدر توفر المعلومات المناسبة وفي الوقت المناسب، يكون دقة القرار وصحته، وتعد المعلومات مصدرًا أساسيًا لصنع القرارات في مجالات الصناعة والتنمية والشئون الاقتصادية والإدارية والعسكرية والسياسية والأمنية[1].

في المجال الأمني لابد من توافر معلومات على مستوى عالي من الدقة والوضوح

(١) حسن علي الزغبي : نظم المعلومات الاستراتيجية، عمان، دار وائل للنشر والتوزيع، الطبعة الأولى، ٢٠٠٥م، ص٥١.

والسرعة لاتخاذ القرارات الأمنية فى المشاكل اليومية المتجددة، ولوضع الاستراتيجيات والخطط الأمنية للفترة القادمة لمواجهة أى خروج على الشرعية محتمل الحدوث، وحتى تصبح المعلومات الأمنية ذات فائدة للعرض على متخذه القرار يراعى فيها توافر بعض الخصائص، ومن أهمها ما يلى:

١- النطاق الزمنى، فقد تكون المعلومات تاريخية أو مستقبلية، وتستخدم المعلومات التاريخية لمتابعة ومراقبة الأداء أو تصميم حلول بديلة لمشاكل روتينية، أما المعلومات المستقبلية تستخدم للتنبؤ بحلول لمشاكل مستقبلية ومعايير رقابية لها.

٢- الشكل الذى تقدَّم فيه المعلومات، فقد تكون ملخصة أو تفصيلية، فالمعلومات الملخصة تعتبر كافية للتعرف على المشكلة، أما المعلومات التفصيلية تستخدم لاتخاذ القرارات فى المستويات القيادية ومراحل اتخاذ القرار.

٣- المعلومات قد تكون متوقعة أو غير متوقعة، والمعلومات المتوقعة تزيد فيها نسبة التأكد طبقًا لدرجة التوقع، والدور الأساسى لنظم المعلومات هو تقديم معلومات غير متوقعة وهى تستخدم لاكتشاف المشاكل من خلال الإنذار المبكر.

٤- مصادر المعلومات، فهناك مصادر داخلية وخارجية. المصادر الداخلية مثل معدلات تنفيذ الأحكام خلال فترة، معدلات ارتكاب جرائم معينة خلال فترة، معدلات ضبط القضايا، أما المصادر الخارجية تمثل بيانات عن المنشآت المهمة فى منطقة ما، أو الشخصيات المهمة فى دائرة معينة، ويجب توافر النوعين من البيانات ولا يكفى الاعتماد على نوع واحد[1].

---

(١) محمد السعيد خشبة : نظم المعلومات المفاهيم والتكنولوجيا، دار الإشعاع للطباعة، القاهرة، ١٩٨٧م، ص٥٥.



٥- درجة تنظيم المعلومات، هناك معلومات منظمة ومعلومات غير منظمة، المعلومات المنظمة تعكس كافة المعلومات التى تحتويها بصورة واضحة ودقيقة، أما المعلومات غير المنظمة فهى تقدم بشكل لا يفصح عما تحتويه من معلومات ولا تساعد متخذ القرار للاستفادة منها.

٦- درجة الدقة فى المعلومات، وتتحدد بما تمثله المعلومات للموقف أو الحدث الذى تصفه وطبيعة المشكلة والعوامل التى تؤثر عليها، وقدرتها على توفير اتجاه معين لدى متخذ القرار.

٧- درجة الرسمية للمعلومات، المعلومات قد تكون رسمية وهى المعلومات التى تخرجها الجهة أو جهات أخرى معتمدة محددة المصدر كالتقارير أو الإحصائيات أو الخطابات الرسمية وتقدمها نظم المعلومات، أما المعلومات غير الرسمية فهى التى تأتى للنظام عن طريق غير رسمى وغير محدد المصدر، أو معتمد من جهة أخرى.

٨- درجة التغير، فالمعلومات قد تكون ثابتة أى غير قابلة للتغيير، ومعلومات قابلة للتغيير، مثال لذلك أسماء الضباط وتاريخ الميلاد ورقم الأقدمية هى معلومات غير قابلة للتغيير وعند حدوث تغيير فيها يشكل خطأ يجب مراجعته، أما الحالة الاجتماعية ومحل الإقامة ومكان العمل فتلك المعلومات قابلة للتغيير.

٩- خاصية المرونة، فالمعلومات ذات قدرة على إعادة التشكيل وإعادة الصياغة، فعلى سبيل المثال يمكن تمثيل المعلومات فى صورة قوائم أو أشكال بيانية أو رسوم متحركة أو أصوات ناطقة.

١٠- قابلية نقلها عبر مسارات محددة لفئة معينة، أو بثها على المشاع لمن يرغب فى استقبالها من خلال شبكات الحاسبات أو وسائل نقل المعلومات المختلفة.

١١- قابلية الاندماج العالية للعناصر المعلوماتية، فيمكن بسهولة تامة ضم عدة قوائم في قائمة أو تكوين نص جديد من فقرات يتم استخلاصها من نصوص سابقة[١].

١٢- خلافًا للموارد المادية التي تنتهي مع الاستهلاك، لا تتأثر موارد المعلومات بالاستهلاك، بل على العكس، فهي - عادةً ما - تنمو مع زيادة استهلاكها لهذا السبب فهناك ارتباط وثيق بين معدل استهلاك المجتمعات للمعلومات وقدرتها على توليد المعارف الجديدة.

١٣- سهولة النسخ؛ حيث يستطيع مستقبل المعلومة نسخ ما يتلقاه من معلومات بوسائل يسيرة للغاية ويشكل ذلك عقبة كبيرة أمام تشريعات الملكية الفكرية الخاصة للمعلومات[٢].

١٤- إمكان استنتاج معلومات صحيحة من معلومات غير صحيحة أو مشوشة، وذلك من خلال تتبع مسارات عدم الاتساق والتعويض عن نقص المعلومات غير المكتملة وتخليصها من الضوضاء.

سادسًا - معايير جودة المعلومات الأمنية :

يقصد بجودة المعلومات الأمنية قدرتها على تحفيز القائد متخذ القرار لاستخدامها ليتخذ موقفًا معينًا أو صدور قرار ما، يتناسب مع ما وفرته هذه المعلومات من اتجاهات معينة لدى متخذ القرار، وجودة المعلومات لا تتحدد بدرجة الدقة والمصداقية الموجودة في المعلومة، ولكن اعتمادًا على وجهة نظر متخذ القرار ومدى رضاه عن تلك المعلومات.

ولتحديد درجة الرضا عن المعلومات هناك ثلاثة عوامل رئيسية يعتمد عليها، وهي:

(1) Bhunia C.T, : Information Technology Network, New AGE, 2005, p45.

(2) O'Brien, James A : Management Information Systems, Third Ed, Chicago: Irwin, 1996, p92.



١ - منفعة المعلومات:

المعلومات يتم تقييمها من زاوية المنافع الأمنية التى تتحقق نتيجة استخدام هذه المعلومات أو نتيجة دورها فى تحفيز الضابط متخذ القرار على استخدامها، ويمكن تحديد المنفعة الأمنية المرتبطة بسهولة الاستخدام وتتضمن أنواع المنافع الآتية[١]:

- المنفعة الشكلية:

يُقصد بها اقتراب شكل المعلومة التى تقدم للضابط لمتخذ القرار مع متطلباته وبصورة تجعلها قابلة للاستخدام الفورى[٢].

- المنفعة الزمنية:

تُقاس تلك المنفعة بتوقيتات توافرها منذ لحظة الاحتياج لها وتتزايد المنفعة الزمنية كلما أُتيحت المعلومات فى توقيتات تسمح بتحليلها واستخدامها فى اتخاذ القرارات الأمنية، والمعلومات التى تتوافر بعد اتخاذ القرار الأمنى، قد يكون لها منفعة فى تصويب القـرارات أو تقليل الآثار السلبية الناتجة عنها[٣].

- المنفعة المكانية:

يُقصد بها سهولة الوصول إلى المعلومة، ففى بعض الأحيان تكون المعلومات متوافرة فى الجهة ويصعب الوصول إليها وقت الحاجة لسوء الحفظ أو لقصور فى التطبيق لاستخراج تقارير وإحصائيات معينة فى حاجة إليها.

- منفعة التملك:

يُقصد بها إدارة المعلومات والتحكم فيها وهى تمثل تملُّك إحدى الإدارات الفرعية

---

(١) إسماعيل محمد محمد السيد: نظم المعلومات لاتخاذ القرارات الإدارية، الإسكندرية، المكتب العربى الحديث للطباعة والنشر، ٢٠٠١م، ص١٠٧.

(2) O'Brien, James A, op. cit, P127.

(٣) طارق طه: نظم المعلومات والحاسبات الآلية من منظور إدارى، القاهرة، دار الفكر العربى، ٢٠٠٨م، ص٩٥.

للمعلومات، وعدم مشاركة تلك الإدارة في اتخاذ القرار أو عرض المعلومات مما يؤثر على تكامل المعلومة لدى الجهة ووجود قصور فيها نتيجة عدم الحصول على كافة المعلومات المتاحة لدى الجهة.

وتتمثل منفعة المعلومات في القيمة التي يتم إضافتها للمستخدم من خلال تلك المعلومات، وبالتالي تؤدي إلى المساعدة في اتخاذ القرارات[١].

٢- درجة الرضا عن المعلومات من قبل القائد متخذ القرار:

تُعد درجة الرضا شيئًا نسبيًا للقائد متخذ القرار، فمن الصعب أن نحكم على القدر الذي ساهمت به المعلومات في عملية اتخاذ القرار، ولكن البديل الذي يمكن عمله هو استخدام مقياس لمدى رضا متخذ القرار عن المعلومات المقدمة إليه، ويرجع ذلك إلى مدى توافر المعلومات المطلوبة لدى متخذ القرار وزمن توفير تلك المعلومات، هل ساهمت المعلومات في توفير معرفة عن المشكلة أو الأزمة لدى متخذ القرار؟ أم أن هناك تأخيرًا في استخراج تلك المعلومات؟ فيتم اتخاذ القرار بدون الاعتماد على تلك المعلومات وهل أسلوب العرض كان مناسبًا وسهلاً ؟ وهل كانت المعلومات واضحة ومباشرة ؟ كل تلك العناصر تؤثر على مدى رضا القائد متخذ القرار[٢].

٣- درجات الخطأ والتحيز في المعلومات:

في اتخاذ القرارات تفضل القيادات جودة المعلومات على كمية المعلومات، وجودة المعلومات تتفاوت باختلاف درجة الخطأ والتحيز، والمشكلة تكمن في أن مستخدم المعلومات لا يكون على علم بدرجة الخطأ أو التحيز، ولا يمكنه إدراك أن هناك خطأ أو تحيز في البيانات، وإلا كان من السهل تعديل تلك المعلومات للقضاء على التحيز.

(١) أشرف السعيد أحمد : تكنولوجيا المعلومات وإدارة الأزمات، القاهرة، ٢٠١٢م، ص٦٧.

(2) O'Brien , James A, op. cit, p116.



والأخطاء تمثل – أيضًا – مشكلة سواء كانت بدون قصد أو متعمدة.

ويرجع وجود خطأ في المعلومات لعدة أسباب من أهمها:

- استخدام طريقة غير دقيقة في جمع البيانات.
- إتباع طريقة غير سليمة في إعداد البيانات في صورة معلومات.
- فقد جزء من البيانات أو ترك بعضها بدون تشغيل.
- الخطأ غير المقصود في إدخال البيانات.
- استخدام ملف خاطئ في حفظ البيانات.
- الخطأ في البرامج المستخدمة لإعداد البيانات باستخدام الحاسب الآلي.
- التزوير المتعمد في البيانات.

هناك عدة طرق تقلل من نسبة الخطأ في المعلومات المتاحة ومنها ما يلي:

- وجود نظام مراجعة على عملية إدخال المعلومات.
- وجود نظام رقابة داخلية على المعلومات لاكتشاف الأخطاء.
- وضع قواعد خاصة بعمليات الإعداد والتجميع للبيانات[1].

العمر الزمني للمعلومات:

يُقصد بالعمر الزمني للمعلومات تلك الخاصية الزمنية المتعلقة بالمعلومات التي يتم تحويلها إلى تقارير وإحصائيات، ويوجد نوعان من تلك البيانات وهي:

- البيانات في تاريخ محدد:

يُقصد بها البيانات التي تتعلق بنقطة زمنية محددة بتاريخ معين مثال لذلك عدد قضايا المخدرات التي تم ضبطها حتى ٢٠١٢/١٢/٣١م.

---

(١) أشرف السعيد أحمد: أثر تكنولوجيا الأزمات على إدارة الأزمة الأمنية (دراسة تطبيقية)، القاهرة، ٢٠١١م، ص ٧٧.

- البيانات عن فترة محددة:

يُقصد بها البيانات التى تعبر عن أى تغير خلال فترة زمنية معينة، مثال لذلك عدد قضايا المخدرات التى تم ضبطها خلال شهر مارس ٢٠١٣م.

ولتوضيح مفهوم العمر الزمنى للمعلومات وقياسه ينبغى أن نتعرض لمصطلحين أساسيين وهما:

فاصل المعلومات الزمنى:

يُقصد به المسافة الزمنية بين تقريرين متتاليين من النوع نفسه، فالتقارير الأسبوعية الفاصل الزمنى لها أسبوع، والتقارير الشهرية الفاصل الزمنى لها شهر، ويرمز إلى الفاصل الزمنى بالرمز (س) (١).

التأخير فى إعداد المعلومات:

يُقصد به التأخير الزمنى الذى يستغرق فى إعداد المعلومات للنشر فى صورة تقرير ويقاس بالفترة الزمنية بين نهاية الفاصل الزمنى للمعلومات وصدور التقرير الجديد للاستخدام، ويرمز للتأخير فى إعداد المعلومات بالرمز (ص).

وباستخدام هذين المصطلحين (فاصل المعلومات الزمنى «س»، التأخير فى إعداد المعلومات «ص») يمكن حساب الحد العمرى الأقصى، والحد العمرى المتوسط، والحد العمرى الأدنى للمعلومات، ويعبر الجدول التالى عن تلك العلاقة:

نوع الحد العمرى للمعلومات	التأخير فى إعداد المعلومات
الحد العمرى الأقصى	ص + س
الحد العمرى المتوسط	ص + ٠,٥ س
الحد العمرى الأدنى	ص

جدول (١-٢) الحد الأقصى والمتوسط والأدنى لعمر المعلومات

(1) Collin, S. M. H : Dictionary of Information Technology, London: Peter Collin Pub, 1996, p141.



يمثل الجدول السابق أسلوب قياس الحد العمرى للمعلومات فى تاريخ معين ومثال لذلك الحد العمرى الأدنى للمعلومات، وتمثل فى زمن التأخير فى إعداد المعلومات، لو كنا بصدد إعداد تقرير عن معدلات تنفيذ الأحكام عن شهر مارس ٢٠١٣م، ومعدل التأخير فى إعداد التأخير هو خمسة أيام وهو وقت تجميع البيانات وإعداد التقرير المطلوب، فإن الحد العمرى الأدنى لصدور التقرير هو ٢٠١٣/٤/٥م، وهو التاريخ المحدد لصدور التقرير فإن زاد على ذلك يكون هناك تأخير فى صدور التقرير، والعمر الأقصى هو معدل التأخير فى إعداد المعلومات ويضاف إليه فاصل المعلومات الزمنى، بمعنى أن هذا التقرير يعد صالحًا للاستخدام حتى تاريخ ٢٠١٣/٥/٥م، وهو تاريخ صدور التقرير التالى عن شهر أبريل.

والعمر الزمنى للمعلومات يمكن التأثير عليه من خلال التغير فى معدل التأخير فى إعداد المعلومات بإتباع أساليب التخزين الحديثة والإدخال المباشر للبيانات واستخراج التقارير مباشرة فعندما نصل إلى درجة تأخير تساوى صفر فإن الحد العمرى للمعلومات سواء الحد الأدنى أو الأقصى تصبح تساوى الفاصل المعلومات الزمنى[1].

سابعًا - تكنولوجيا المعلومات وصنع القرار الأمنى :

جوهر العمل فى مجال الشرطة هو صنع القرارات، فالعمل الشرطى يحتاج إلى اتخاذ قرارات يومية عديدة فى مواقف مختلفة، والقائد الناجح يتوقف نجاحه على مدى قدرته على صنع القرار، وهو اختيار بين عدة بدائل استجابة لموقف معين، كتحديد قوة أمنية لكمين شرطى، أو تحديد موقع معسكر قوات أمن واختيار بين عدة بدائل مختلفة لكل منها مميزات وعيوب مختلفة، ويتوقف نجاح القيادة على مدى فاعليتها فى اتخاذ قرارات فعالة ورشيدة، لإحداث التغيير داخل المنظمة فى أدائها لوظائفها،

(1) Collin, S. M. H, op. cit, p143.

والفاعلية ليست قدرة فطرية ولكن يمكن اكتسابها وتنميتها، ولذا يتم إلقاء الضوء على طبيعة عملية اتخاذ القرارات ومراحل صنع القرارات.

دور نظم وتكنولوجيا المعلومات فى صنع القرار الشرطى :

تعمل تكنولوجيا المعلومات فى الجهات الشرطية على تخفيض عدد قنوات الاتصال، بين القائد ومرؤوسيه (الاتصالات الهابطة)، وبين المرؤوسين والقائد (الاتصالات الصاعدة)، أو بين المستوى الإدارى الواحد (الاتصالات الأفقية)، مع القدرة على انتشار أوسع فى المشاركة بالمعلومات ما بين المستويات الإدارية المختلفة فى ظل تباعد المسافات ، والاستعانة بالأشخاص الذين يمتلكون الخبرة لإضافة المعلومات التى يحتاجها صانع القرار، فلا يوجد فى المنظمة مستويات إدارية متعارضة، ولكنها تكون متكاملة ويؤدى تطبيق تكنولوجيا المعلومات لتطوير نظم المعلومات الأمنية المستخدمة، وتوزيع المهام بدقة وتدفق المعلومات المطلوبة إلى صانعى القرار الأمنى فى الوقت المناسب.

وهناك عدة مهام نعمل من أجلها، وهى :

١- سهولة العمل الذى يهدف إلى دعم جميع المشاركين فى العمل الشرطى بإمدادهم بمخرجات ذات جودة عالية وفاعلية كبيرة.

٢- زيادة قدرة رجال الشرطة على حل المشاكل وبناء العلاقات وحسن الود مع الجمهور.

٣- زيادة تحقيق أنشطة منع الجرائم والقدرة على عمل التحريات وأعمال البحث الجنائى وتحقيق نتائج إيجابية فى تقليل أعمال الإخلال بالأمن العام.

٤- تحقق كم أكبر من المعرفة لرجال الشرطة مما يساعد على التعرف على مسببات الجرائم والعمل على منعها والقضاء عليها.



٥- استخدام أجهزة وشبكات الاتصال الحديثة المعتمدة على الحاسب الآلى تؤدى إلى سرعة استجابة قوات الشرطة للحادث وأيضًا سرعة رد الفعل عند التعامل مع الحادث.

٦- باستخدام تكنولوجيا المعلومات فإن قاعدة المعرفة ستكون متاحة لجميع العاملين فى المجال الشرطى (حسب قواعد الأمن المتبعة وهى المعرفة على قدر الحاجة) وذلك يحقق عدم مركزية امتلاك البيانات والمعلومات مما يؤدى إلى سهولة اتخاذ القرارات.

٧- يتم الاستعانة بنظم المعلومات الجغرافية للاستفادة من ربط قاعدة البيانات العادية بالبيانات الجغرافية للمساعدة فى اتخاذ القرار.

يتضح مما سبق أهمية الدور الذى تلعبه المعلومات فى عملية صنع القرارات، وأهمية أن تتوافر هذه المعلومات فى التوقيت والشكل المناسبين، فضلاً عن دقتها وارتباطها الوثيق بموضوع القرار الذى يصدر من جانب رجل الإدارة.

أسباب الفشل فى عملية صناعة القرار الشرطى:

يتوقف نجاح القائد فى عمله على نوعية القرارات التى يتخذها، فقد تؤدى القرارات غير الرشيدة إلى أن يكتشف بعد فترة أنه لا يقوم بأعمال كان يجب القيام بها، أو أنه غير قادر على القيام بأعمال يجب القيام بها الأمر الذى يخلق شعورًا بالإحباط والاستياء نتيجة فشله فى عمله[1].

(1) Owen, Jo : **The Leadership Skills Handbook**, London; Philadelphia: Kogan Page,2006, p59.

ويرجع السبب فى فشل القرار الشرطى - غالبًا - إلى ما يلى:

١ - الفشل فى إعطاء الأوزان المناسبة للأولويات:

قد يرجع السبب فى عدم سلامة القرارات المتخذة إلى عدم قدرة المدير على تحديد الأولويات المتعلقة بموضوع المشكلة والإخفاق فى تحديد أهمية العوامل المختلفة والأوزان المقررة لكل منها[١].

٢ - تأجيل اتخاذ القرارات بلا مبرر:

بعض القيادات لا تقوم باتخاذ القرار فى الوقت المناسب، فعندما يقول المدير سوف أفكر فى الأمر فيما بعد، أو أنا مشغول جدًا الآن، فى كل تلك الأحوال يكون هناك اتخاذ قرار، وهو تأجيل اتخاذ القرار، ولا يدرك أنه يتخذ قرارًا فعلاً[٢].

٣ - الاهتمام المتزايد بالتفاصيل:

وذلك حينما يهتم المديرون بتفاصيل الموضوعات، وتتولد قناعة لديهم بأنهم مطالبون باتخاذ كل القرارات بأنفسهم ولا يعطون حرية للمستويات الأقل فى اتخاذ القرارات الخاصة بهم.

٤ - تهدئة الموقف الحرج:

بعض القيادات تبنى قراراتهم على الظروف المحيطة بهم، فلو أدت إحدى المشكلات إلى احتدام الموقف، فإن المدير يتخذ القرار الذى يؤدى إلى تهدئة الموقف، وإرضاء الأطراف المتذمرة، وقد يترتب على ذلك تراكم المشكلة الأصلية نتيجة لعدم اهتمامه بها وبحلها، واهتمامه بالأمور العرضية التى تسبب إزعاجًا لسير العمل، وغالبًا ما ينتج

(١) عبد الحكم أحمد الخزامى، فن اتخاذ القرار مدخل تطبيقى، مكتبة ابن سينا للنشر والتوزيع والتصدير، القاهرة: ١٩٩٠م، ص٥٧.
(2) Owen, Jo, op.cit, p65.



عن هذه القرارات الوقتية سلسلة من المشكلات تظهر فيما بعد[1].

٥- الإفراط في استخدام معيار الصواب والخطأ:

بعض القيادات يحاولون الوصول إلى تحليلات كاملة للموقف، ولا تكون هذه المجموعة على استعداد لاتخاذ القرار إلا عندما تتضح أمامها الرؤية الكاملة لكل متغيرات ومحددات الموقف، ولهذا فإنها تشعر بصعوبة بالغة في تحديد الصواب والخطأ، وقد يؤدي هذا الاتجاه إلى عدم الوصول إلى قرارات إدارية سليمة، نظرًا لأن متغيرات المواقف الإدارية المختلفة لا تتضمن بالضرورة جوانب صحيحة مطلقة أو جوانب سلبية مطلقة.

٦- التفاؤل المبني على التخمين:

بعض القيادات يثقون بخبراتهم في اتخاذ القرارات الصائبة بدرجة كبيرة، وقدراتهم على الإحساس بالنتائج عن طريق التخمين وليس الدراسة، وهم -غالبًا- أصحاب نجاحات كثيرة في مجال اتخاذ القرارات، ربما لأنهم كانوا يعتمدون في بداية حياتهم العملية على البيانات الواقعية في اتخاذهم للقرارات، أو نجاح وليد الصدفة والظروف، وعندما تقدموا في مجالهم الوظيفي وشغلوا مناصب قيادية وزادت مشاغلهم، اعتمدوا على النجاحات السابقة، والقدرة على التخمين والتوقع ولم يقوموا بالجهود السابقة نفسها في البحث عن الحقائق اللازمة لاتخاذ القرارات[2].

٧- النظرة الضيقة للأمور:

إن المنظمة نظام متكامل، ومهما كان القرار الذي يتخذ ويبدو أنه متعلق بأمور مستقلة، كأن يخص قسمًا أو إدارة ما أو نشاط معين فهو في النهاية يؤثر ويتأثر بباقي الأقسام والإدارات والأنشطة، وبعض القيادات تكون نظرتهم للأمور ضيقة ويعتبرون أنفسهم بمعزل

(1) Fletcher, Keith, op.cit, P117.

(2) Fletcher, Keith ,op.cit, P118.

عن بقية أجزاء المنظمة، ويعجزون عن إدراك كل الجوانب اللازمة لاتخاذ القرار، وغالبًا ما يواجهون بمشاكل فيما بعد عندما يتطلب الأمر منهم مواجهة المتغيرات العديدة التى يتطلبها اتخاذ القرار.

معوقات اتخاذ القرار الشرطى:

تتعدد وتتنوع المشاكل التى تواجه اتخاذ القرار الشرطى، وهذه المعوقات والمشاكل إما إدارية أو بيئية أو ترجع إلى طبيعة العمل الشرطى ومن أهم تلك الأسباب(1):

١- المركزية فى سلطة اتخاذ القرارات وعدم تفويض السلطة لاتخاذ القرارات دون الرجوع للقيادات الأعلى.

٢- عدم وضوح الأهداف الأمنية والخطط وسريتها لدى بعض القيادات الشرطية قد يجعل الرؤية غير واضحة ومكتملة أمام صانع القرار فى عمليات التنبؤ.

٣- عدم إحساس بعض القيادات بالاطمئنان والأمان عند اتخاذهم القرارات خوفًا من المسئولية لكثرة اللوائح والقرارات والأوامر الدورية، والخوف من عدم الإلمام بها يؤدى إلى الإحجام عن اتخاذ القرار والرجوع إلى رؤسائهم فى كل كبيرة وصغيرة لأخذ الموافقة على اتخاذ القرار للاطمئنان إلى صحة وسلامة القرارات وانسجامها مع سياسية الوزارة والقيادات.

٤- تشابك العلاقات والمصالح فى المشكلة أو الموقف الذى يواجهه ضابط الشرطة ويصعب التعرف على الأبعاد المختلفة.

٥- بعض القيادات يبنون قراراتهم على الظروف المحيطة بهم، بمعنى أنه لو أدت إحدى الأزمات إلى احتدام الموقف، فإن القائد يتخذ القرار الذى يؤدى إلى

(1) Rosenthal,Uriel, Pijnenburg, Bert : Crisis Management and Decision Making, Dordrecht ; Boston :Kluwer Academic Publishers,1991, P93.



تهدئة الموقف وإرضاء الأطراف المتذمرة، ويترتب على ذلك تراكم المشكلات الأصلية نتيجة لعدم الاهتمام بها وبحلولها والاهتمام المطلق بالأمور العرضية التى تسبب إزعاجًا لسير العمل، وغالبًا ما ينتج عن هذه القرارات الوقتية سلسلة من المشكلات والأزمات[1] .

٦- عدم وجود معيار ثابت يمكن به قياس رشد القرار؛ حيث إن رشد القرار يختلف من شخص إلى آخر ولو تم اتخاذ القرار فى الظروف نفسها وذلك لنسبية عملية تقييم نتائج القرار وهل حقق القرار أهدافه كاملة أم ناقصة ؟

٧- التأخير فى اتخاذ القرارات بلا مبرر لدى بعض القيادات وتأجيل اتخاذ القرار ظنًا منهم انتهاء الأزمة، وأنها سوف تحل دون التدخل.

٨- بعض القيادات يثقون بدرجة كبيرة بخبراتهم وقدراتهم على الإحساس وتوقع النتائج عن طريق التخمين والشعور الداخلى.

٩- تنوع وتباين الجهات التى تحدث بها أزمات، وتعدد تلك الجهات تحتاج إلى تنسيق فى اتخاذ القرار والمواجهة ودراسات عديدة، فى ظل عدم وفرة المعلومات المتكاملة اللازمة لاتخاذ القرار.

ثامنًا - مدى الحاجة لتكنولوجيا المعلومات فى العمل الأمنى :

تظهر أهمية تكنولوجيا المعلومات ومدى الحاجة إليها فى المجالات الأمنية المختلفة وبصفة خاصة فى مجال إدارة الأزمات الأمنية، وطبيعة العمل الشرطة هناك أزمات أمنية مختلفة وبصفة الدوام وقد تكون يومية، وهناك الحاجة إلى معلومات سريعة ودقيقة وصحيحة ومحدثة وعرضها بأسلوب مناسب، فطبيعة إدارة الأزمات تعتمد

(١) أشرف السعيد أحمد: أثر تكنولوجيا المعلومات على إدارة الأزمة الأمنية، مرجع سابق، ص ١٢٦ وما بعدها.

على اتخاذ قرار سريع، والقرار يعتمد على المعلومات المتاحة، فكلما توافرت معلومات بصورة سريعة كان القرار سريعًا، وكلما كانت المعلومات دقيقة وصحيحة كان القرار صائبًا ومن أهم أسباب الحاجة لتكنولوجيا المعلومات ما يأتى:

١ - الحاجة إلى السرعة فى الحصول على المعلومات:

حتى نتمكن من عرض المعلومات المطلوبة بالسرعة المناسبة يراعى توافر نظام معلومات تتوافر فيه البيانات المختلفة للحصول على المعلومات المطلوبة فى أى مجال أمنى أو يتعلق بإدارة الأزمات الأمنية وتوافر من المصدر المباشر لها.

٢ - الحاجة إلى معلومات دقيقة :

أثناء المشكلات الأمنية نلاحظ التسابق فى عرض كم هائل من البيانات والمعلومات، مما قد يحدث شيئًا من عدم الدقة أو تعارض فى المعلومات، مما يؤدى إلى إضاعة وقت ومجهود فريق إدارة البحث فى فرز تلك المعلومات، والتحقق من صحتها. وعرض معلومات غير مطلوبة تؤدى إلى عدم التركيز، والدخول فى مشاكل أخرى فرعية لا علاقة لها بالمشكلة الحالية، مما يوضح لنا مدى أهمية الحاجة إلى الدقة فى المعلومات.

٣ - الحاجة إلى معلومات حديثة:

يتم جمع البيانات من جهات عديدة داخل نظام المعلومات، ونلاحظ -أحيانًا- أن تلك البيانات لا يتم تحديثها إلا عند الحاجة إليها، مما يضيع الوقت فى عملية التحديث، وعدم الاعتماد وفقد الثقة بنظام المعلومات الحالى؛ حيث إن المعلومات الناتجة عنه قد تكون غير صحيحة لعدم تحديث قاعدة البيانات.

٤ - الحاجة إلى أسلوب مناسب لعرض المعلومات:

يعد أسلوب عرض المعلومات من أهم العوامل المؤثرة فى اتخاذ القرار؛ حيث إن



عرض المعلومة بأسلوب ما، قد يؤدى إلى تحول القيادات إلى اتجاه مختلف، وهنا تظهر عملية التهوين والتهويل، التى تعد من أكبر المشاكل فى أسلوب عرض المعلومات؛ حيث يتعمد القائم بعرض الأزمة تهوين الموقف خوفًا من المسئولية، أو تهويل الموقف للظهور بمظهر القائد القوى المسيطر المتحكم أمام قياداته.



الفصل الثالث

استراتيجية أمن المعلومات



الفصل الثالث
استراتيجية أمن المعلومات

تمهيد:

إن التطور الهائل الذي يعيشه العالم في تقنية المعلومات، يحتم على كل دولة ومجتمع مواكبة هذا التطور والعمل على اكتمال حلقات منظومة المعلوماتية بدءًا بالأنظمة ومرورًا بالبنية التحتية، وانتهاءً بالكوادر الوطنية المؤهلة، وقد شملت تلك التقنية قطاعًا واسعًا من وسائل نقل وتخزين وبث المعرفة، فكان لابد من تأمين شبكة المعلومات من الاختراق، ووضع استراتيجية وسياسة لتأمين للمعلومات. لكل منشاة أسلوبها الخاص في توفير الأمن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات التي تم تحديدها وإمكاناتها المادية والميزانية المخصصة للحماية، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية ولا مبالغًا بها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، معالجة أوجه القصور والمعوقات، والعمل على تطوير تقنية المعلومات.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي :

أولاً : مفهوم أمن المعلومات.

ثانيًا : مفهوم الاستراتيجية.

ثالثًا : محل الحماية.

رابعًا : المخاطر المحتملة.

خامسًا : أهم أساليب تأمين قواعد البيانات.

أولاً- مفهوم أمن المعلومات :

إن التطورات الحديثة فى تقنية المعلومات أحدثت تغيرات مستمرة بأساليب العمل فى كثير من المجالات وكافة نواحى الحياة المختلفة، وأصبحت عملية انتقال وتوصيل المعلومات عبر الشبكات المحلية والدولية من الأمور الروتينية فى عصرنا الحالى وإحدى علامات العصر المميزة التى لا يمكن الاستغناء عنها لتأثيرها الواضح فى تسهيل العديد من الخدمات ومتطلبات الحياة العصرية، وقلّة كلفة استعمالها عما كانت عليه، فى ظل عصر الثورة المعلوماتية والتقدم العلمى الكبير، ما زالت القرصنة الإلكترونية مشكلة تؤرق وتهدد الجميع لما لها من تداعيات وخيمة على سلامة المجتمع وأمنه، فهناك تطور سريع فى عمليات الاختراق وتقنيات وأساليب القراصنة، وأصبحت هذه التقنية الحديثة للمعلومات سلاحًا ذو حدين تحرص المنظمات على اقتناءه وتوفير سبل الحماية من الاختراق وتحديد الاستراتيجيات والإجراءات الدفاعية والوقائية من الاختراق أو التخريب، فكان لأمن المعلومات الأهمية الكبرى فى الحفاظ على تلك التقنية من الخطر المدمر لها.

أمن المعلومات (Information Security) :

مع تزايد القيمة الاقتصادية للمعلومات وتطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة عبر الشبكة من موقع لآخر زاد الاهتمام بأمن نظم المعلومات والاتصالات بشكلٍ مهم للغاية؛ حتى أصبحت تلك النظم تمثل عاملاً رئيسيًا فى إدارة جميع القطاعات المختلفة، ووجب العمل على توفير الحماية التقنية لها، وتوفير وسائل تقنية متنامية كجدران النار وكلمات السر ووسائل التعريف البيولوجية والتشفير وغيرها.

ويعرَّف أمن المعلومات بأنه هو العلم الذى يبحث فى نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التى تهددها ومن الاعتداء عليها، والعمل على تحديد

الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية أثناء التداول لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان صحة هذه الاتصالات[1].

وتعد النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات، ويجب الحفاظ على العناصر الرئيسية لأمن المعلومات المتمثلة في السرية وسلامة المحتوى والاستمرارية وعدم إنكار التصرف، وفيما يلي سنتعرض لكل منها بالتفصيل المناسب.

السرية أو الموثوقية (Confidentiality) :

السرية تعني ذلك المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالإطلاع عليها أو الكشف عنها، أي التأكد من أن المعلومات لا يتم الإطلاع عليها من قِبل أشخاص غير مصرح لهم بذلك طبقًا للصلاحيات الأمنية المحددة، وتحديد الصلاحيات المحددة لكل مستخدم ومناطق الاستخدام المسموح الدخول عليها، وأيضًا التوقيت المصرح له بالتواجد خلاله على الشبكة، وأيضًا حماية بيانات المستخدم من الإفشاء والاطلاع عليها دون إذن أو تخويل من مدير النظام.

على سبيل المثال، بطاقة الائتمان والمعاملات التجارية على شبكة يتطلب رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة، يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الأماكن ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، والنسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها، أما إذا كان الطرف غير المصرح به قد حصل

(١) أشرف السعيد أحمد : مقدمة في علوم الحاسب ، القاهرة ، ٢٠١١م،ص٢٢٢.



على رقم البطاقة بأى شكل من الأشكال، وبذلك فقد تم انتهاك مبدأ السرية فى حفظ وتخزين البيانات، والسرية أمر ضرورى لكنها غير كافية للحفاظ على الخصوصية من الناس الذين يخترقون الأنظمة لسرقة المعلومات.

التكاملية وسلامة المحتوى (Integrity) :

فى مجال أمن المعلومات سلامة المحتوى تعنى الحفاظ على البيانات التى يتم تداولها من خلال الشبكة صحيحة ولم يتم تعديلها أو العبث بها بالتغيير من الأشخاص الغير مخول لهم بذلك، ولم يتم تدمير المحتوى أو تغيره أو العبث به فى أية مرحلة من مراحل المعالجة أو التبادل سواء فى مرحلة التعامل الداخلى مع المعلومات أو عن طريق تدخل غير مشروع، عندما يقوم شخص بقصد أو بغير قصد انتهاك سلامة أو إضرار أو حذف ملفات البيانات المهمة وهو غير مخول له بذلك فهذا انتهاك لسلامة البيانات، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو إتلافها فهذا انتهاك سلامة بيانات، وعندما يكون الموظف قادرًا على تعديل راتبه فى قاعدة البيانات والمرتبات، وعندما يقوم مستخدم غير مصرح له بتخريب موقع على شبكة الإنترنت.

استمرارية توفر المعلومات أو الخدمة (Availability) :

التأكد من استمرار عمل نظام المعلومات والقدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، أن تكون المعلومات متوفرة عند الحاجة إليها، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو الوصول إليها، إذ لا يكفى الوجود بل يتعين ضمان الاستمرارية وتقديم الخدمة، و العمل على توافر نظم عالية السرية تهدف إلى استمرارية الحماية فى جميع الأوقات، ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائى، أو تعطل الأجهزة، أو نظام الترقيات والتحديث، والتأكد من أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات، والضوابط الأمنية

المستخدمة لحمايته، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح[1].

عدم إنكار التصرف المرتبط بالمعلومات (Non- Repudiation) :

ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفًا ما قد تم من شخصٍ ما في وقت معين، والقدرة على إثبات شخصية الطرف الآخر على الشبكة وإثبات شخصية المستخدم.

وأبسط أنواع الحماية هو استخدام نظام التعريف بشخص المستخدم ومشروعيته وهذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من الشخص المخول بالاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية والتي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه البيولوجي المفاتيح المشفرة ويمكن أن نضم إلى هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

ثانيًا- مفهوم الاستراتيجية :

مصطلح الاستراتيجية يعد من المصطلحات القديمة المأخوذ من الكلمة الإغريقية (Strato) وهي تعني الجيش أو الحشود العسكرية، ومن تلك الكلمة اشتقت اليونانية القديمة مصطلح (Strategos) وتعني فن إدارة وقيادة الحروب، وظهرت الاستراتيجية في اللغة الإنجليزية (Strategy) بقصد التخطيط للعمليات العسكرية قبل نشوب الحروب، وفي الوقت نفسه فن إدارة تلك العمليات عقب نشوب الحروب.

وبالرغم من أن أصل الكلمة (Strategy) يعود إلى التعبير العسكري، إلا أنها تستخدم

---

(١) أشرف السعيد أحمد : القرصنة الإلكترونية، القاهرة، ٢٠١٢م، ص٩٠.



الآن بكثرة فى سياقات مختلفة مثل استراتيجيات العمل، استراتيجيات التسويق، وتعكس الاستراتيجية الخطط أو الطرق أو الأساليب المحددة مُسبقًا لتحقيق هدف معين على المدى القريب أو البعيد فى ضوء الإمكانيات المتاحة، واعتمادًا على استخدام التخطيط والإجراءات المتوفرة التى يمكن الحصول عليها فى المدى القصير.

أهداف الاستراتيجية :

تهدف الاستراتيجية إلى تحقيق هدف رئيسى تعمل من أجله سياسة المنظمة من خلال الاستخدام الأمثل لكافة الإمكانات والوسائل المتوفرة للوصول إليه، وقد يكون الهدف سياسيًا أو اقتصاديًا أو عسكريًا أو معنويًا وقد يكون صغيرًا محدودًا أو كبيرًا.

وللوصول إلى الهدف الرئيسى قد يتم وضع مجموعة من الأهداف المرحلية التى يؤدى تحقيقها إلى الهدف الاستراتيجى، وهذه الأهداف هى ما تسمى بالأهداف الاستراتيجية المرحلية، غير أن جميع الأهداف تشترك فى كونها جميعًا تسعى وتعمل من أجل تحقيق الهدف الرئيسى الذى عين وحدد سلفًا من قبل السلطة السياسية العليا للمنظمة.

وسائل الاستراتيجية :

تتباين الوسائل التى تستخدمها الاستراتيجية لتحقيق هدفها تبعًا للتباين فى طبيعة وأهمية ذلك الهدف وتبعًا للإمكانات والقدرات المتاحة للظروف والأجواء المحلية والدولية السائدة، والاستراتيجية الناجحة هى التى توفق إلى اختيار الوسيلة أو الوسائل الأجدى بين كافة الوسائل المتاحة للوصول إلى هدفها، أى التى تنجح فى تحقيق وتأمين التوافق بين الوسيلة والهدف وفى خلق التأثير النفسى الكافى لزعزعة ثقة الخصم بنفسه وحرمانه من حرية العمل مما سيؤدى إلى حماية المنظمة من تهديداته.

ولكي يكون اختيار الوسيلة ناجحًا فمن الضرورى عمل دراسة واعية للموقف بشتى جوانبه لمعرفة العدو المطلوب قهره وتمييز نقاط ضعفه الأكثر حساسية مع تحليل عميق للتأثيرات الحاسمة التى يمكن أن تحدثها السياسة المختارة على معنويات الخصم وهذا يقتضى إنشاء مخطط استراتيجي يتضمن كافة الأعمال الممكنة وردود الأفعال المتوقعة عليها محليًا ودوليًا لوضع الحلول المناسبة ليكون المخطط الاستراتيجى مترابط الأجزاء قادر على مواجهة أية مفاجآت أو ردود فعل غير ملائمة أو سيئة التأثير لضمان حرية العمل للخطة الاستراتيجية.

معايير استخدام مصطلح الاستراتيجية :

هناك معايير أساسية يجب أن تتوافر فيما يتصف بالخطة الاستراتيجية، وسنتعرض لأهمها فيما يلى :

١- مستوى التخطيط و الأهداف (الغايات) :

يقوم التخطيط بتحديد أهداف تسمى الغايات أو أهداف عليا بعيدة المدى، وهى أهداف يطلق عليها الأهداف الاستراتيجية وبناءً عليها يتم تخصيص المهام اللازمة لتحقيق هذه الأهداف، ومن ثَمّ ينتقل التخطيط إلى مستوى التخطيط التعبوى والذى يحدد بدوره أهدافًا لتحقيق مهمته وتتصف بأنها أهداف متوسطة المدى أو الأهداف الفرعية والمناطق ويطلق عليها الأهداف التعبوية والتى تترجم بدورها إلى مهام تُكلَّف بها الوحدات الميدانى، ومن ثَمّ ينتقل مستوى التخطيط إلى تخطيط عال المعايير يقوم بتحديد أهداف تخطيطية وهى أهداف مباشرة أو أهداف صغرى، ثم تتحول تلك الأهداف إلى مهام تكلف بها كل وحدة صغرى على حدة، وفى الغالب تحول هذه الأهداف إلى مستوى رابع على مستوى الفرد والقائد وهو ما يسمى الهدف المباشر، ونلاحظ أن تسلسل الخطط وتدرجها يتم من أعلى المستوى الإدارى أو القيادى إلى

أسفله ، وهناك فصل بين المستويات يكون ضرورى ومحسوم لما له من مميزات تفويض السلطة وتخصيص المهام وتوفير الأعباء الذهنية والتركيز فى إنجاز وتحقيق المهام وتوفير قنوات الاتصال والسيطرة.

٢- وجود تهديدات أو منافسة :

يرتبط مصطلح استراتيجية بوجوب وجود تهديدات ما، فالاستخدام العسكرى لا يستخدم إلا فى حالة وجود تهديدات تجبر المجتمعات على تكوين الجيوش، أما المنظمات غير العسكرية لا تستخدم هذا المصطلح للتخطيط لأعمالها إلا أنها تستخدم مصطلحات أخرى مثل، المنهج أو التخطيط الإدارى إذا ما كان هناك هدفًا أو مجموعة أهداف تريد تحقيقها، وفى تلك الحالة لا يوجد تهديدات ومعوقات مباشرة تمنع تحقيق هذا الهدف، وتكون خطة المنظمة عبارة عن منهج ثابت ومباشر فى سبيل تحقيق هذا الهدف، فالمنهج أو الخطة الإدارية ما هى إلا خطوات وخطط ثابتة فى سبيل تحقيق هدف محدد، وأيضًا يمكن تقسيمه إلى مستويات تخطيطية عليا، ومستوى متوسط أو برامج أو إدارى، ومستوى تنفيذى، لا حاجة لها لتكوين استراتيجية ومناورات، وفى مجال أمن المعلومات نجد أن هناك خطر أو تهديد وهو يتمثل فى عملية القرصنة الإلكترونية، واختراق قواعد البيانات، والهدف حماية البيانات من كافة الأساليب غير المشروعة للدخول عليها.

٣- أعلى مستوى إدارى أو قيادى :

ينحصر استخدامات مصطلح استراتيجية فى كل ما يعده أو يخططه أو يتداوله المستوى القيادى أو الإدارى الأعلى فى أية منظمة، ويكون ذلك المستوى هو المسئول عن تحديد وتحقيق غايات المنظمة، وهو المعروف بالمستوى الذى يشترك فيه فريق عمل مكون من جميع قادة الأنشطة بصرف النظر عن حجمها ودورها فى التنظيم.

٤- تخصيص المهام وتحديد المسؤوليات :

كثيرًا ما نستخدم مصطلح استراتيجية فى حياتنا العامة وحتى العلمية نقلاً عن الغرب دون مراعاة لمدلول هذا المصطلح، فالخطة الاستراتيجية يجب أن ينتج عنها تقسيم للأهداف وتخصيص للمهام وتوزيع للأدوار لمستويات المتوسطة والدنيا، وتبعًا لهذه المهام تعد تلك المستويات خطط جديدة ومنفصلة لتحقيقها والتى بمجموع نجاحها يتحقق الهدف، وإن لم تتواجد تلك الخطط الدنيا فلا مجال لوصف الخطة بالاستراتيجية لفقدها عنصر تقسيم الأدوار والتعاون وبالتالى فقد القدرة على المناورة.

ومن هذه المعايير نلاحظ أن مصطلح الاستراتيجية لا يفضل استخدامه إلا إذا ارتبط بخطة يضعها أعلى مستوى إدارى بالهيكل التنظيمى للمنظمة وبشرط ارتباط الخطة المباشر بتحقيق غايات أو أهداف عامة رئيسية المنظمة وبشرط وجود تهديدات خارجية أو قوة تنافسية مما يستوجب معها استخدام أساليب المناورة أو الاعتماد على تحليل للفرص والتهديدات كما هو فى علوم الإدارة، ولا يصح استخدام مصطلح (الاستراتيجية) مع أى موضوع لا تتوافر فيه تلك المعايير سواء على المستوى الإدارى أو العلمى.

أهداف استراتيجية أمن المعلومات :

تهدف استراتيجية أمن المعلومات إلى :

- تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وفى مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة استرجاعها.
- تهدف الاستراتيجية إلى تحديد الإلكترونية التى يتم من خلالها تحقيق وتنفيذ

الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر[1].

- بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بها بذلك.

ثالثاً - محل الحماية :

محل الحماية هنا - بصفة أساسية - البيانات فهي الهدف الأساسي لأمن المعلومات، ويتمثل أمن المعلومات في مجموعة من الآليات والإجراءات والأدوات التي تستخدم للوقاية أو للتقليل من المخاطر والتهديدات التي تتعرض لها أجهزة الحاسبات الآلية والشبكات وقواعد البيانات، وهي متعددة من حيث الطبيعة والغرض، ومحور الخطر على المعلومات هو الإنسان، سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بنظام المعلومات، فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، أو شخص غير مصرح له بالدخول على النظام وقام بعملية اختراق والدخول على نظام المعلومات[2].

تنصب المخاطر والاعتداءات على بيئة وأمن المعلومات في أربع نقاط أساسية، وهي: أمن البيانات والمعلومات، متمثلة في قواعد البيانات المختلفة الموجودة على الشبكة، أمن النظام والتطبيقات والبرامج ونظم التشغيل، الأمن المادي للأجهزة والمكونات المادية، أمن الشبكة والدخول إلى الأنظمة، وهي تشكل مكونات تقنية المعلومات، وكل منها يشمل

(١) يونس عرب : **الخصوصية وأمن المعلومات** ، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي - اتحاد المصارف العربية، ٢٠ - ٢٢ أيار ٢٠٠١ ، عمان - الأردن، ٢٠٠١م.

(2) Karl De Leeuw, J. A. Bergstra : The History of Information Security, A Comprehensive Handbook, Elsevier, 2007, p212.

قواعد ومتطلبات تختلف عن الأخرى ويتعين أن تكون أنظمة الأمن فى هذه المواضع متكاملة مع بعضها؛ حتى تحقق الوقاية المطلوبة.

١ - أمن البيانات والمعلومات (أمن قواعد البيانات):

وهى تمثل الدم الحى للأنظمة، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم، والمعطيات قد تكون فى طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط تخزين خارجية، ويتم اختراق شبكات المعلومات وقواعد البيانات وأجهزة الخادمات الرئيسية للجهات الحكومية أو الشركات بدون تصريح دخول.

٢ - أمن النظام (البرامج والتطبيقات ونظم التشغيل):

أمن النظام يقصد به التطبيقات التى يتم التعامل من خلالها على الشبكة وعدم السماح لأشخاص غير مصرح لهم بالدخول على التطبيق، والتطبيقات هى مجموعة من الأوامر التى يتم كتابتها فى نسق معين لإنجاز الأعمال، وقد تكون مستقلة عن النظام أو مخزنة فيه ذاته، وتقوم بأعمال محددة، ويقصد بأمن النظام تلك العملية التى يتم من خلالها التأكد من مستخدم التطبيق، هل مسموح له بالاستخدام ومدى الصلاحيات الممنوحة له، ويمكن تحديد مستويات الحماية طبقًا لسرية وخطورة البيانات، يمكن تحديد جهاز معين فقط لكل مستخدم، وأيضًا يمكن تحديد ساعات معينة فقط يستطيع الدخول على التطبيق فيها وخلاف ذلك لا يسمح له باستخدام التطبيق.

٣- التأمين المادى للأجهـزة:

التأمين المادى للأجهزة، ويقصد به تأمين المكونات المادية للنظام من أجهزة ومعدات من العبث بها ضد السرقة أو التلف، وهى تمثل كافة المعدات والأدوات المادية التى يتكون



منها النظام، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وكل المكونات المادية للنظام أو الشبكة؛ حيث يتم اختراقها والعبث بما تحويه من معلومات لسهولة اختراقها وعدم وجود الحماية الكافية.

٤- تأمين شبكة الاتصالات (الولوج أو الدخول إلى الأنظمة):

محل الحماية لأمن الشبكة هو عملية الاتصال وتبادل البيانات والمعلومات بين أجهزة الحاسب الآلي بالشبكة والنظام النهائي سواء كان نظام المستضيف (الخادم) وبين جهاز حاسب آلي آخر على الشبكة، ويهدف أمن الشبكات توفير وسائل الحماية في تعامله مع الشبكة، وشبكات الاتصال التي تربط أجهزة التقنية بعضها في بعض محليًا أو دوليًا، تتيح فرصة اختراق النظم من خلالها والتعرف على البيانات والمعلومات أثناء انتقالها من حاسب لآخر أو عند إدخال بيانات سرية في وثيقة مثل رقم بطاقة الضمان وكلمة السر.

رابعًا - المخاطر المحتملة:

هناك العديد من المخاطر المحتملة التي يمكن أن تواجه نظام المعلومات ويخشى منها، وتتركز تلك المخاطر في عملية اختراق أمن المعلومات والوصول إلى المعلومات والبيانات بطريقة غير مشروعة وبدون تصريح لذلك عن طريق ثغرات في نظام الحماية الخاصة بقواعد البيانات أو شبكات الحاسبات، واستغلال تلك نقاط الضعف بسبب القصور في إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية أو معنوية، كالحصول على كلمات السر أو معلومات عن النظام عن طريق غير مشروع، والقيام بأنشطة غير مصرح له بها، وتلك الثغرات تعد من أهم المخاطر التي تهدد أمن المعلومات؛ حيث لا يمكن ذكر المخاطر على سبيل الحصر، ومن أبرزها ما يلي:

١ - وسائل الأمن المتعلقة بالتعريف بشخص المستخدم ومشروعيته:

هى تلك الأساليب التى تهدف إلى ضمان التحقق من أن الشخص الذى يقوم باستخدام النظام أو الشبكة هو ذلك الشخص المصرح له بهذا الاستخدام وفقًا للصلاحيات الممنوحة له، متمثلة فى الدخول على البيانات بالإطلاع أو الإضافة أو التعديل، وذلك من خلال اسم المستخدم وكلمة السر بأشكالها المختلفة، متمثلة فى الدخول على النظام أو التطبيقات، والبطاقات الذكية المستخدمة للتعريف بالشخص والسماح له بالدخول إلى أماكن لا يُسمح فيها بالدخول إلا لأشخاص محددين وفى أوقات محددة، أو وسائل التعريف البيولوجية التى تعتمد على سمات معينة فى شخص المستخدم متصلة ببنائه البيولوجى كبصمة اليد أو الصوت أو بصمة العين، والمفاتيح المشفرة، والأقفال الإلكترونية التى تحدد دخولها لأشخاص بذاتهم[1].

٢- الوسائل المتعلقة بالتحكم بالدخول والنفاذ إلى الشبكة:

هذه الوسائل تعمل على الحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، والتأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة، ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن الاستخدام غير المصرح به، والتعديل غير المصرح به، والإتلاف غير المصرح به، وإصدار المعلومات والأوامر غير المصرح بها ولهذا فإن خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق التخويل والتثبت منه.

٣- مجموعة الوسائل التى تهدف إلى تحقيق سرية المعلومات:

هذه الخدمات تحمى المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعنى بشكل عام إخفاء المعلومات من خلال تشفيرها أو من خلال وسائل

(1) Ohn R. Vacca : Computer and Information Security Handbook, Morgan Kaufmann, C2009, p245.



أخرى كمنع التعرف على حجمها أو مقدارها أو الجهة المرسلة إليها، وإجراءات حماية نسخ الحفظ الاحتياطية، والحماية المادية للأجهزة ومكونات الشبكات.

٤- وسائل الحماية التكاملية :

هذه الخدمات تهدف إلى حماية مخاطر تغيير البيانات وضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك، أثناء عمليات إدخالها أو معالجتها أو نقلها وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو التحوير أو إعادة تسجيل جزء منها أو غير ذلك وتهدف هذه الوسائل أيضًا إلى الحماية من أنشطة تدمير المعطيات بشكل كامل أو إلغائها دون تخويل باستخدام برامج الكشف عن الفيروسات(١).

٥- إنكار الخدمة:

يتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته على احتمالها أو توجيه عدد كبير من عناوين الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسلة فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه.

٦- عدم الإقرار بالقيام بالتصرف :

يتمثل هذا الخطر في عدم إقرار الشخص المرسل إليه أو المرسل بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصيًا الذي قام بإرسال طلب الشراء عبر الإنترنت، وتهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار انه هو الذي

(1) Paulus R. Wayleith: Data Security: **Laws and Safeguards**, Nova Science Publishers, C2008, p76.

قام بالتصرف، وهى وسائل ذات أهمية بالغة فى بيئة الأعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل فى الوقت الحاضر على تقنيات التوقيع الإلكترونى وشهادات التوثيق الصادرة عن طرفٍ ثالث.

٧- وسائل مراقبة الاستخدام وتتبع سجلات النفاذ :

وهى التقنيات التى تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذى قام بالعمل المعين فى وقتٍ معين، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التى تحدد الاستخدام.

٨- الاعتداء على حق التخويل :

يتم ذلك من خلال قيام الشخص المخول له استخدام النظام لغرضٍ ما باستخدامه فى غير هذا الغرض دون أن يحصل على التخويل بذلك، وهذا الخطر يعد من الأخطار الداخلية، إساءة استخدام النظام من قِبل موظفى المنشأة، وقد يكون أيضًا من الأخطار الخارجية، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به أو استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع أو من جزء مشروع ومن ثَمَّ القيام بأنشطة غير مشروعة[1].

٩- زراعة نقاط الضعف :

عادة ينتج هذا الخطر عن اقتحام من قِبل شخص غير مصرح له بذلك أو من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد، ومن أشهر أمثلة ذلك زراعة المخاطر حصان طروادة، وهو عبارة عن برنامج يؤدى غرضًا مشروعًا فى الظاهر لكنه يمكن أن يستخدم فى

(1) L.Jean Camp, Stephen Lewis: Economics of Information Security, Springer, C2004, p163.



الخفاء للقيام بنشاط غير مشروع، كان يستخدم برنامج معالجة كلمات ظاهريًا لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام.

١٠ - مراقبة الاتصالات :

بدون اختراق كمبيوتر المجني عليه يتمكن الجاني من الحصول على معلومات سرية غالبًا ما تكون من المعلومات التي تسهل له مستقبلاً اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها.

١١ - اعتراض الاتصالات :

كذلك بدون اختراق النظام يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي[1].

خامسًا - أهم أساليب تأمين قواعد البيانات :

تأمين قواعد البيانات والحفاظ عليها من المخاطر السابق الحديث عنها، ومنع الدخول غير المشروع إلى شبكات الحاسب، والوصول إلى أجهزة الشركة دون رغبتهم أو علمهم، بالإضافة إلى الأضرار المادية والمعنوية الجسيمة التي قد يحدثها عند إتلافه أو الإطلاع أو سرقة بيانات أو ملفات أو صور خاصة.

هناك عدة أساليب لتأمين قاعدة البيانات تتمثل في البرمجيات المختلفة للحفاظ

(1) Tyler Moore: Economics of Information Security and Privacy, Springer, C2010, p127.

على معلوماتك آمنة، كاستخدام برمجيات لمكافحة الفيروسات والاختراقات، وأيضًا استخدام برامج أو أجهزة الجدار النارية للمنع من الاختراق، بالإضافة إلى الأساليب التقنية في المحافظة على البيانات والمعلومات وسلامة المحتوى بإتباع أسلوب التشفير، وسنتناول أهمها على النحو التالي:

أ- برمجيات كشف ومقاومة الفيروسات :

هي البرامج التي تقوم بحماية الأجهزة من هجمات الفيروسات التي تشكل تهديدًا أمنيًا على أمن البيانات، يمكنها رصد مصدر هذه البرامج في القرص الصلب أو الأقراص المدمجة، أو وحدات الحفظ الخارجي، أو الرسائل الإلكترونية، في حالة اكتشاف الفيروس تعمل هذه البرمجيات على مسح أو تعطيل عمله.

وتعد تقنيات مضادات الفيروسات الأكثر انتشارًا، إلا أن هناك ثغرات في فهم دور هذه المضادات للفيروسات التي تصيب النظام، وما قد ينتج من الاستخدامات الخاطئة لها على أداء وفعالية النظام، وسنتعرض لماهية الفيروسات، والبرامج الخاصة بمكافحة الفيروسات، ونشأتها، وكيفية عملها.

ما هي الفيروسات ؟

فيروس الحاسب الآلي هو عبارة عن برنامج صغير يتم إدخاله على الحاسب الآلي بدون علم المستخدم وتسبب أمور غير متوقعة وأشياء ضارة وغير مرغوبة بغرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآلي، أو لتسهيل عملية الدخول غير المشروع للنظام[1]. يقوم من أنشأ الفيروس ببرمجته وتوجيه الأوامر الخاصة له بتحديد التوقيت الذي يبدأ فيه الفيروس بالنشاط وعادةً ما تعطي فرصة كافية من الوقت

(١) أشرف السعيد أحمد : **مقدمة في علوم الحاسب**، القاهرة، ٢٠١١م، ص١٦٦.



للفيروس؛ حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات فى النظام، تختلف الفيروسات من حيث بدأ النشاط فهناك من يبدأ بتاريخ أو وقت محدد، وهناك من يبدأ بالعمل بعد تنفيذ أمر معين فى البرنامج المصاب وهناك من يبدأ بالنشاط بعد التكاثر والوصول إلى رقم معين من النسخ، وبعد أن ينشط الفيروس يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس، فهناك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك أنواع أخرى تقوم بحذف أو تعديل بعض الملفات، وهناك من يقوم بتكرار ونسخ نفسه؛ حتى يشل جهازك تمامًا وأنواع أخرى تقوم بمسح كل المعلومات من القرص الصلب.

البرامج المضادة للفيروسات (Virus countermeasures) :

برامج مكافحة الفيروسات هى البرامج التى تستخدم لحماية الأجهزة من هجمات الفيروسات وبقية البرامج التى تشكل تهديدًا أمنيًا على المعلومات، وتستطيع أن تحدد هذه الملفات الضارة القادمة من أى مصدر مثل الأقراص المدمجة والأقراص اللينة والرسائل الإلكترونية وكذلك يمكنها رصد هذه البرامج فى القرص الصلب، وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط، بل هو اصطلاح يطلق على هذا النوع من البرمجيات. وفى كثير من الأحيان يطلق على كل البرامج الضارة اسم فيروس بغض النظر عما إذا كان فيروس فعلاً أو دودة أو (Trojan Horse) أو أى نوع آخر من أنواع البرمجيات الضارة[1].

وتتمكن هذه البرامج من مسح أو تعطيل عمل البرامج المهددة لسلامة الجهاز وملفات البرامج الموجودة على جهاز الحاسب ويتكون برنامج مضاد الفيروسات من

(1) Tyler Moore, Op.Cit, P145.

جزئيين مختلفين:

١- التشغيل المباشر عند الدخول :

وهذا الجزء يعمل تلقائيًا عند تشغيل (الدخول) للبرامج أو تحميل الملفات من الإنترنت وهو ما يعرف (On Access Element) .

٢- التشغيل عند الطلب :

وهذا الجزء يعمل عندما تطلب أنت منه ذلك، وهو متخصص بالكشف عن الفيروسات وأحصنة طروادة (TORJAN) فى القرص الصلب والأقراص اللينة والأقراص المدمجة وهو ما يُعرف (Demand Element).

هناك تسابق مستمر بين مطورى البرامج الضارة وبرامج مضادات الفيروسات، فكلما وجِد برنامج فعَّال لمكافحة الفيروسات الحالية، يتم إنتاج نوع جديد من الفيروسات لا يعالجها البرنامج الحالى.

العلاج الناجح للفيروسات هو منعها أو عدم السماح لها بالدخول لنظام الحاسب إلا أن تحقيق ذلك يعد من الصعوبة بمكان، ولكن إذا حدثت الإصابة بالفيروس فهناك إجراءات يمكن اتخاذها فى مواجهة الفيروس أو لمعالجته وتقليل عواقبه وهى عبارة عن خيارات يتم اختيار الأنسب منها والذى يوفر أعلى حماية وأقل تكلفة[1].

نشأة برمجيات مكافحة الفيروسات :

عقب ظهور الفيروسات كانت بداية قيام بعض الشركات فى تصميم برامج مكافحة الفيروسات لحماية أجهزة الحاسب الآلى، ومع السباق السريع فى تصميم وتطوير الفيروسات التى كانت بسيطة فى بداية ظهورها، أصبح هناك تعقيدًا كبيرًا طرأ على

(1) Karl De Leeuw, J. A. Bergstra, Op.Cit, P95.



برامج مكافحة الفيروسات لمواجهة تطور الفيروسات بشكل سريع، ويمكن تقسيم المراحل والأجيال التى تطورت خلالها برامج مكافحة الفيروسات إلى ما يلى :

الجيل الأول - الماسحات البسيطة (Simple Scanner)،

كانت بداية ظهور برمجيات مكافحة الفيروسات مع أول ظهور للفيروسات بسيطة نظرًا لبساطة الفيروسات وسهولة التعرف عليها وكانت تلك البرمجيات كانت تعتمد على بعض النقاط البسيطة وغير المعقدة لاكتشاف الفيروسات والقضاء عليها وتعتمد تلك البرامج فى هذه المرحلة على ما يلى:

- يحتاج برنامج مكافحة الفيروسات علامة معينة(Signature) للتعرف من خلالها على الفيروس.
- فى بعض أنواع برنامج مكافحة الفيروسات يتم الاعتماد على قياس حجم الملف وأكتشاف التغير فى الطول نتيجة التصاق الفيروس به[1].

الجيل الثانى - الماسحات الموجهة (Heuristic Scanner) ،

وهى تتميز بالآتى:

- استخدام طرق موجهة للبحث عن الإصابات المتوقعة.
- بعضها يبحث عن كود فيروسى معين داخل الملفات فإذا وُجد؛ فهذا يعنى إصابة الملف المحدد.
- ويمكن -أيضًا- اختبار صحة الملفات (Integrity) باستخدام قيمة الـ(Checksum) الموجودة مع الملفات فإذا كان الفيروس قد عَدَّل الملف دون أن يُعدل قيمة الـ(Checksum) فإن البرنامج المضاد للفيروسات سيكتشف

(١) أشرف السعيد أحمد : مقدمة فى علوم الحاسب ، مرجع سابق، ص ١٦٦.

أن هناك إصابة، نسبة لاختلاف قيمة (Checksum) المخزنة مع بيانات الملف[1].

الجيل الثالث - الماسحات البسيطة (Activity Trap)،

فى تلك النوعية من البرمجيات يتم اكتشاف فيروسات الذاكرة بالأفعال التى تقوم بها فى النظام وليس بتركيبها كما فى الجيل السابق.

الجيل الرابع - الحماية الكاملة (Full-featured protection)،

هذا الجيل من التقنية تستخدم كل التقنيات السابقة فى حزمة واحدة وتحتوى مقدرات كبيرة تحد من انتشار الفيروسات ونشاطها التخريبى.

كيفية عمل البرامج المضادة للفيروسات :

البرامج المضادة للفيروسات عبارة عن تقنية مسح ورصد للبرامج المشبوهة التى تتميز بخصائص معينة أو تحتوى على صيغة معينة من البرمجة عبارة عن مجموعة من الأرقام الثنائية وهى التى تعرف بـ (التوقيع) ويتم ذلك بالطريقة التالية:

يقوم البرنامج المضاد بتحديد كل الملفات والبرامج ذات الطبيعة التنفيذية، ويتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة فى قاعدة المعلومات الخاصة بالبرنامج المضاد للفيروسات، بعد عملية المقارنة يقوم البرنامج المضاد باكتشاف الفيروس أو حصان طروادة ويقوم بإخطار المستخدم عنه، يقوم البرنامج المضاد بتخيير المستخدم بين مسح أو تعطيل الفيروس أو بإصلاح الخلل بطريقة آلية، ويتم ذلك من خلال مرحلتين :

(1) Karl De Leeuw, J. A. Bergstra, Op.Cit, P144.



المرحلة الأولى - اكتشاف الفيروس (Virus Detection):

هى تحديد حدوث الإصابة بالفيروس وتحديد مكانه، ويتم التعرف على نوع الفيروس الذى سبب الإصابة (Identification) عقب اكتشاف الإصابة، وذلك من خلال علامات معينة فى كود الفيروس أو بسلوكه الذى يقوم به فى النظام؛ حيث يقوم مصنعو ومبرمجو الفيروسات - عادةً - بتعديل أو تحريف التوقيع الأصلى لبعض البرامج الشهيرة وذلك لتضليل المستخدم والبرنامج الأصلى وتقوم تكنولوجيا الكشف عن هذا التزوير والتعديل بواسطة المقارنة السريعة بين التوقيعات الأصلية والمزيفة.

المرحلة الثانية - إزالة الفيروس (Virus Removal):

بعد التعرف على نوع الفيروس تتم إزالته من الملف المصاب وإرجاع الملف إلى وضعه الأصلى وتَعَقُّب كل النسخ الأخرى من الفيروس للحد من انتشاره مرةً أخرى، إذا أسفرت مرحلة الاكتشاف عن وجود فيروس لم يتم التعرف على نوعه يجب اللجوء لخيار التخلص من البرنامج المصاب، ثم إعادة تركيبه مرة أخرى باستخدام النسخ الاحتياطية.

مفاهيم خاطئة عن برامج الحماية من الفيروسات:

لعل من أكثر المفاهيم الخاطئة بين المستخدمين على مستوى العالم هى الاعتقاد بأن اقتناء برنامج مضاد للفيروسات يمنع ويحمى من هجوم الهاكرز والمخترقين وهذا طبعًا ليس صحيح؛ حيث إن هذه البرامج تحمى فقط من الفيروسات والديدان وتستطيع التعرف على معظم أحصنة طروادة ولكن لا تقوم بغلق المنافذ والمعابر الموجودة فى جهاز الحاسب الآلى والتى تمكن المخترقين من الوصول إلى الجهاز والمعلومات.

مدى الاعتمادية على هذه البرامج :

ليس هناك برنامج مضاد للفيروسات قادر على تقديم حماية كاملة لجهاز الحاسب الآلي، وعند القيام بالتحديث المستمر لبرنامج مكافحة الفيروسات -بصفة مستمرة- سوف تحصل على حماية تصل إلى ٩٥٪، لظهور أنواع جديدة من الفيروسات لم يتمكن البرنامج من اكتشافها؛ حيث تعمل هذه البرمجيات بأسلوب رد الفعل -دائمًا- الفيروسات تتقدم بالجديد ويأتي التحديث لمحاولة اكتشاف تلك الفيروسات والقضاء عليها.

ب- الجدار الناري (Fire Wall) :

هي عبارة عن أجهزة (Hardware)، أو برامج (Software)، وتعمل على فلترة وتصفية حركة البيانات الواردة والصادرة من وإلى الشبكة اعتمادًا على قوانين ومعاملات بسيطة، وتطورت الجدران النارية بشكل كبير منذ نشأتها، ويعد أول استخدام لها لتحقيق الأمن في أوائل التسعينات، وكان عبارة عن موجهات لبروتوكول (IP) للتحقق من هوية المستخدمين، باستخدام أسلوب اسمح للمستخدم الفلاني بالدخول والنفاذ إلى الملف التالي، أو امنع المستخدم فلان (أو برنامج معين) من الدخول إلى المنطقة (أو المناطق) التالية[1].

وكانت هذه الجدران النارية فعَّالة ولكنها محدودة؛ حيث كان من الصعب فلترة البيانات، وتحديد أجزاء التطبيقات المراد منعها من النفاذ إلى الشبكة، وفي أحيان أخرى كانت عناصر الشبكة، مثل الموظفين العاملين ضمنها، تتغير، مما كان يستدعي تغيير القوانين، وجاءت الأجيال التالية من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل وأدى ذلك إلى المزيد من الابتكارات، ليس فقط في مجال تسريع أداء الجدران

(1) Kimberly Kiefer: **Information Security**: A Legal, Business, and Technical Handbook, American Bar Association, C2004, p37.



النارية وتقديم خدماتها، بل وأيضا فى تضمينها قدرات متعددة فى التعامل وإجراء التعديلات المطلوبة، وتتمثل هذه القدرات فى ما يلى [1]:

١ - التحقق من هوية المستخدمين :

بداية التطوير فى الجدران النارية كان من حيث القدرات القوية للتحقق من الهوية، وإذا كانت السياسيات الأمنية التى تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة من شبكة خارجية مثل الإنترنت، فظهرت الحاجة إلى استخدام أسلوب للتحقق من هوية المستخدمين، ويقصد بالتحقق من الهوية هو التأكد من صحة شخصية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتى لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين؛ حيث إن أسماء المستخدمين وكلماتهم السرية يمكن نسخها وإعادة استخدامها، أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية، أو برمجيات حساب الشفرات الرقمية الخاصة، وبواسطة الشهادات الرقمية يمكن تفادى هجمات إعادة الاستخدام؛ حيث يتم نسخ اسم المستخدم وكلمته السرية وإعادة استخدامها للنفاذ إلى الشبكة.

٢ - وسائل مراقبة الاستخدام وتتبع سجلات الدخول والخروج للشبكة (Logging and Monitoring) :

وهى التقنيات التى تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذى قام بعمل المعين فى وقت محدد، ومراقبة العمليات التى قام بها هذا الشخص، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التى تحدد الاستخدام مثل (Log File) و(Edit Records)، تشمل أيضًا برامج مراقبة الشبكة، وهى تعد إضافة كبيرة للجدار النارية والاختراقات.

(1) Indira Carr: Computer Crime International Library of Criminolgy, Criminal Justice and Penology- Second Series Ashgate,, C2009, P167.

٣- الشبكات الافتراضية الخاصة (Virtual Private Networks) :

وتعد الإضافة الثالثة إلى الجدران النارية هى التشفير البينى للجدران النارية (Firewall - to Firewall) والتى تعرف بالشبكات الافتراضية الخاصة (Virtual Private Networks)، وسُميت هذه الشبكات بالخاصة لأنها تستخدم التشفير، وسميت بالافتراضية الخاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة.

رغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام المودمات (Modems) والموجهات (Routers) للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية، وهى جيل جديد من الجدران النارية يحتوى على عدد من التقنيات بما فى ذلك حلول جدران نارية جاهزة، بمعنى أنها لا تحتاج إلى إعداد من قبل المستخدم ويمكن البدء باستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل أو البنية التحتية المستخدمة، وانتقلت وسائل حماية الإنترنت من مستويات الحماية الفردية، التى تقوم على وضع وسائل الحماية ومنها الجدران النارية فى المنطقة التى تفصل الشبكة الخاصة عن الموجهات التى تنقل الاتصال إلى الشبكة العالمية (الإنترنت)، إلى مستويات الأمن المتعددة والتى تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات أو نظم المعلومات داخل الشبكة الخاصة، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل للنظام(1).

٤- مراقبة المحتوى (Content Screening) :

يقصد به تحليل محتويات الحزم (Packets) الواردة للشبكة ومعرفة واختبار محتواها، وخلال الأعوام القليلة الماضية أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة

(1) Kimberly Kiefer, Op.Cit, P54.



المحتوى الوارد إلى الشبكة للبحث عن الفيروسات والبرمجيات الضارة، ومراقبة عناوين الإنترنت.

أهمية استخدام الجدار الناري:

تقوم أجهزة وبرمجيات الجدار النارى بالعمل على حماية وعزل التطبيقات والخدمات والأجهزة من الشبكة الداخلية من حركة المرور غير المرغوب فيها القادمة من الإنترنت العامة، والحد من أو تعطيل الوصول من المضيفين من الشبكة الداخلية لخدمات الإنترنت العامة، كما -أيضًا- تعمل على دعم ترجمة عنوان الشبكة (NAT)، والذى يسمح للشبكة الداخلية لاستخدام عناوين (IP) الخاصة ومشاركة اتصال واحد على شبكة الإنترنت العامة (إما مع عنوان (IP) واحد أو مجموعة مشتركة من العناوين العامة تعيينه تلقائيًا).

ويعد تركيب جدار حماية نارى أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الحاسب الآلى قبل الدخول إلى الإنترنت للمرة الأولى، وتختلف الجدران النارية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصى هو الخيار المناسب. وفى حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافى لجدار النار فى الشبكة لتصفية جميع الحركة المرورية. وكثير من الشبكات والخوادم تأتى مع نظام جدار نار افتراضى، ولكن ينبغى التأكد فيما إذا كان يقوم بعمل تصفية فعَّالة لجميع الأشياء التى تحتاج إليها، فإن لم يكن قادرًا على ذلك، فينبغى توفير جدار حماية نارى أقوى منه، وبعض أنظمة التشغيل تحتوى على حماية نارى، مثل ويندوز اكس بى مع الحزمة الخدمية/الإصدار٢ (Service Pack2)ونظام التشغيل ماكنتوش(MacOS X).

ج- التشفير (Encryption) :

يعرف التشفير بأنه عملية ترميز البيانات وتحويل المعلومات إلى شفرات غير مفهومة تبدو غير ذات معنًى ليتعذر قراءتها من أي شخص غير المرخص لهم من الاطلاع على تلك البيانات والمعلومات أو فهمها، أي أنها عملية الحفاظ على سرية البيانات والمعلومات باستخدام برامج لها القدرة على تحويل وترجمة تلك البيانات والمعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قِبل أشخاص غير مخول لهم بذلك لا يمكنهم فهم أي شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة، على اختلاف أنواع وأشكال البرامج المتخصصة في هذا المجال إلا أنها جميعًا تتشارك في القاعدة أو الأساس وهي مبنية على مفهوم بسيط؛ حيث يقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس، ويجعل التشفير المعلومات في جهاز الحاسب الآلي غير قابلة للقراءة من قِبل أي شخص يستطيع أن يتسلل خلسة إلى الجهاز دون إذن، ويتم ذلك باستخدام بروتوكول تشفير الشبكات اللاسلكية (WEP) [(1)].

وتحظى تقنيات وسياسات التشفير باهتمام كبير في مجال أمن المعلومات؛ حيث تمثل حماية التشفير الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية، التكاملية، توفير المعلومات، فالتشفير يعمل على تحقيق توفير وحماية هذه العناصر، فضمان سرية المعلومات أصبح يعتمد على تشفير وترميز الملفات والمعطيات، بل تشفير وسائل التحقق من المستخدم، وكلمات السر، كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتأكد لدى فك التشفير أن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل أو التغيير، ويعد التشفير بوجه عام وتطبيقاته العديدة، من أهم الوسائل لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية.

(1) Karl De Leeuw ,J .A .Bergstra ,Op.Cit ,P164.



والتشفير يتم من خلال مرحلتين رئيستين، المرحلة الأولى تتمثل فى تشفير النص على نحو يحوله إلى رموز غير مفهومة، أو رموز مقروءة بلغة غير مفهومة، والمرحلة الثانية تتم عقب استلام الرسالة وتتمثل فى فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء، وهذه المسالة تقوم بها برمجيات التشفير التى تختلف أنواعها ووظائفها(١).

أنواع تكنولوجيا التشفير :

هناك نوعان من التكنولوجيا المستخدمة فى التشفير وهى التشفير المتناظر والتشفير غير المتناظر (Symmetric Algorithms and Asymmetric Algorithms).

والفرق بينهما بسيط جدًا ولكنه مهم جدًا فى مستوى ودرجة الأمن؛ حيث إن التشفير المتناظر يتم بتشفير الرسالة أو المعلومات باستخدام الرقم العام وكذلك فى الوقت نفسه يتم فك الشفرة وترجمة المعلومات إلى وضعها الأصلى باستخدام الرقم العام نفسه (٢).

ولذلك لو كان هناك شخص آخر يعرف هذا الرقم أو حصل عليه من الدليل العام فإنه قادر على فك الشفرة و قراءة تلك الرسالة أو المعلومة، أما إذا ما تم تشفير المعلومات بأسلوب (غير المتناظر) فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذى تمت على أساسه عملية التشفير، أما من حيث طرق التشفير، فثمة التشفير الترميزى، والتشفير المعتمد على مفاتيح التشفير، التى قد تكون مفاتيح عامة أو خاصة أو مزيجًا منها.

(1) Paulus R. Wayleith, Op .Cit, P94.

(2) Ohn R. Vacca, Op.Cit, P97.

ويتم تطبيق هذا المبدأ فى مجال التشفير من خلال إصدار رقم الأساس عن طريق البرنامج المتخصص أو إحدى الهيئات المستقلة والمتخصصة فى إصدار هذه الأرقام وهو ما يعرف بـ(Certificate Authority) (CA)، بحيث يكون لكل مستخدم رقم أساس وهو (ع) ويتم تقسيم هذا الرقم إلى مجموعتين (س) وهو ما يعرف بالمفتاح العام و(ص) هو ما يعرف بالمفتاح الخاص، بحيث إذا قمنا بعملية ضرب (س X ص) يكون الناتج هو (ع) الرقم الأساس وهو الرقم اللازم لإعادة الملفات والمعلومات إلى وضعها الأصلى قبل التشفير وطبعًا هذا الرقم محمى ومشفر بقوة ولا يمكن الوصول إليه بسهولة.

المفتاح العام (Public Key) :

المفتاح العام هو ذلك الرقم الذى يتم تداوله ونشره بين بقية المستخدمين لتشفير أية معلومات أو رسالة إلكترونية مخصصة ويعتبر رقمك العام أساس عملية التشفير ولا يستطيع أحد فك رموز تلك المعلومة غيرك أنت، لأنها تحتاج إلى الرقم السرى وليكن هو المفتاح الخاص بك لإكمال العملية الحسابية والوصول إلى الرقم الأساس وبالتالى فتح الملفات مرة أخرى.

المفتاح الخاص (Private Key) :

المفتاح الخاص هو النصف الآخر المكمل للمفتاح العام للوصول إلى الرقم الأساس وإعادة المعلومات المشفرة إلى وضعها الطبيعى قبل التشفير، وهذا المفتاح هو الذى يميز كل شخص عن غيره من المستخدمين ويكون بمثابة هوية إلكترونية تمكنُ صاحبها من فك أية معلومة مشفرة مرسلة إليه على أساس رقمه العام ولذلك يجب عليك الاحتفاظ بالمفتاح الخاص سرًا، و بهذه الطريقة لا يستطيع أحد فك الشفرات وقراءة المعلومات المحمية بهذه الطريقة دون اكتمال الحلقة و التى لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام والمفتاح الخاص.



الفصل الرابع

تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية

الفصل الرابع
تكنولوجيا المعلومات الامنية والحكومة الإلكترونية

تمهيد:

تعد وزارة الداخلية من أولى الوزارات التي أخذت بنهج التطور الإلكترونى والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية بل والتقدم والتطور فى هذا المجال لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية فى مصر، وتعد الإدارة الإلكترونية فى وزارة الداخلية من أحد المحركات الأساسية والفعّالة فى إدارة الحكومة الإلكترونية المصرية، وتقدم وزارة الداخلية خدماتها عبر الموقع الخاص بوزارة الداخلية على شبكة الإنترنت العالمية، بالإضافة إلى بعض الخدمات على موقع بوابة الحكومة الإلكترونية المصرية التى تُبث عبر شبكة الإنترنت.

وفى ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتى:

أولاً: مفهوم الحكومة الإلكترونية.

ثانيًا: تطبيقات وزارة الداخلية المصرية فى مجال الحكومة الإلكترونية.

ثالثًا: تكنولوجيا المعلومات الأمنية فى مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية.

أولاً - مفهوم الحكومة الإلكترونية :

يتسم العمل الحكومى فى معظم دول العالم بإجراءاته الروتينية الطويلة وبالبطء العام، وهذا يُشكل تكلفة كبيرة على الدول من حيث الجهد المبذول، وعدم استغلال الموارد المتاحة على الوجه الأمثل، ومع تطور التقنيات الحديثة وثورة المعلومات اتجه العالم بأكمله نحو تبنى الوسائل الحديثة المتمثلة فى استخدام تكنولوجيا المعلومات والاتصالات وخصوصًا الإنترنت للوصول إلى حكومات أفضل.

ويعد مفهوم الحكومة الإلكترونية أحد الطرق الحديثة والمتطورة التى تتعامل بها حكومات الدول لاستخدام التقنية الحديثة فى تحسين كفاءة المؤسسات والأجهزة الحكومية واستغلال الموارد المتوفرة داخل الدولة بالشكل الأفضل، لتزويد المواطنين بآليات أفضل وأسرع وأيسر للوصول إلى المعلومات والخدمات داخل مؤسسات الدولة والعمل على توحيد المعلومات الحكومية وترتيبها وتنظيمها، وتتيح للمواطنين المشاركة بآرائهم ومقترحاتهم لدى المؤسسات الحكومية.

وتعرف الحكومة الإلكترونية بأنها «استخدام تكنولوجيا الاتصالات والمعلومات لتحقيق الإصلاح من خلال تسريع عملية الشفافية، وتقريب المسافات، وإزالة العوائق، وإعطاء الفرصة للمواطنين للمشاركة فى كافة مراحل العملية السياسية والقرارات المتعلقة بها والتى تؤثر على نواحى حياتهم المختلفة»[1].

أهداف برنامج الحكومة الإلكترونية:

لا يقتصر مفهوم الحكومة الإلكترونية على كونه تغييرًا فى أسلوب العمل يتم بمقتضاه إجراء المعاملات نفسها بصورة إلكترونية، ولكنه يشكل نمطًا وشكلاً جديدًا للحكومة بمفهومها التقليدى من خلال تبسيط الإجراءات وتحسين الخدمات الحكومية وإعادة

(١) رأفت رضوان : **الحكومة الإلكترونية** ،القاهرة، المركز الدولى للدراسات المستقبلية و الاستراتيجية، ٢٠٠٥م، ٢٢ ص.

تنظيم الأجهزة الحكومية، وتسهيل الوصول إلى الخدمات الحكومية عن طريق إتاحة عدد كبير من الخدمات الحكومية عبر بوابة الحكومة المصرية، وعبر قنوات جديدة مثل شبكات الهاتف المحمول، مراكز الاتصال، منافذ الخدمات الجماهيرية والشباك الواحد، والعمل على توفير خدمات حكومية جديدة.

تبسيط الإجراءات عن طريق إجراءات إصدار التصاريح (السياحية، الصناعية، المحاكم ... إلخ)، وصميم الخدمات الحكومية من منظور المواطن، إتاحة خدمة التوقيع الإلكترونى، تقديم وسائل جديدة لسداد الرسوم مثل (بطاقات الائتمان، السداد عند التسلُّم، عن طريق الهاتف المحمول وخلافه).

دعم شفافية الجهات الحكومية عن طريق نشر نتائج التوظيف، ميكنة إجراءات إصدار التصاريح، وإرسال إخطارات إلى بوابة المشتريات الحكومية عن طريق الهاتف المحمول.

ومن أهم أهداف الحكومة الإلكترونية ما يلى[1]:

١ - تقديم الخدمات إلى المواطنين فى مكان وجودهم:

تعد تقديم الخدمات الجماهيرية للمواطنين فى أماكن تواجدهم من أهم أهداف الحكومة الإلكترونية والتى تسعى إلى زيادة قدرة الحكومة على توفير المعلومات والخدمات العامة للمستفيدين بتكلفة أقل، وسرعة ودقة فى إنجاز المعاملات وخدمات الجمهور، بطريقة متواصلة ومفيدة للمواطنين بالشكل والأسلوب المناسبين مع تطوير أفضل الطرق لمشاركتهم فى العملية التنفيذية، ويتم التعامل الإلكترونى فى الخدمات الحكومية من خلال ميكنة هذه الخدمات بصورة تحقق إمكانية الحصول على الخدمات

(١) فريد النجار: الحكومة الإلكترونية، بين النظرية و التطبيق، الإسكندرية، الدار الجامعية، ٢٠٠٨، ص ٢٤١.



دون الحاجة إلى الانتقال إلى مقر أداء الخدمة من خلال[1]:

- التعرف على إجراء ومتطلبات الحصول على الخدمة.
- إتاحة وتوفير النماذج المستخدمة في أداء الخدمة.
- فتح قناة اتصال بين الأفراد والجهات الحكومية.

٢- تحسين أداء المؤسسات الحكومية من خلال ما يلي :

- تخفيض الإنفاق الحكومي والتكاليف المباشرة عن طريق الاستخدام الأمثل للموارد واستحداث آليات جديدة، وخفض تكلفة الخدمات بصورة فعّالة[2].
- الانفتاح على العالم الخارجي وتوفير مناخ مشجع للمستثمرين، وتذليل العقبات التي يواجهونها والتي تتمثل بشكل أساسي في بطء الإجراءات وتعقيدها، مما سينعكس بشكل إيجابي على تشجيع الاستثمار المحلي وجذب المزيد من الاستثمارات الأجنبية، وتقديم الخدمات لهم وتبسيط الإجراءات الحكومية في أقل وقت ممكن.
- رفع كفاءة أعمال الجهاز الحكومي والمراقبة والمتابعة من خلال خفض دورة الوقت المرتبطة بإنتاج وتقديم الخدمات الفورية.
- تحقيق التنسيق بين المؤسسات الحكومية مع بعضها البعض؛ حيث التشابك والاعتماد المتبادل في المعاملات والذي يؤدي إلى التعقيدات الإدارية التي تؤدي إلى بطء الإجراءات.

---

(١) خالد ممدوح إبراهيم : أمن الحكومة الإلكترونية، الإسكندرية، الدار الجامعية، ٢٠٠٨م، ص٦٥.

(٢) فريد النجار، مرجع سابق ، ص ٢٢٦.

- تهيئة الجهاز الحكومى للاندماج فى النظام وتحقيق مستوى أداء يتواكب مع النظم الحديثة المتبعة فى الدول المتقدمة.

- توفير معلومة دقيقة محدثة لمتخذ القرار وذلك للمعاونة فى التخطيط طويل المدى، المشروعات التنموية، متابعة التنفيذ بشكل دقيق.

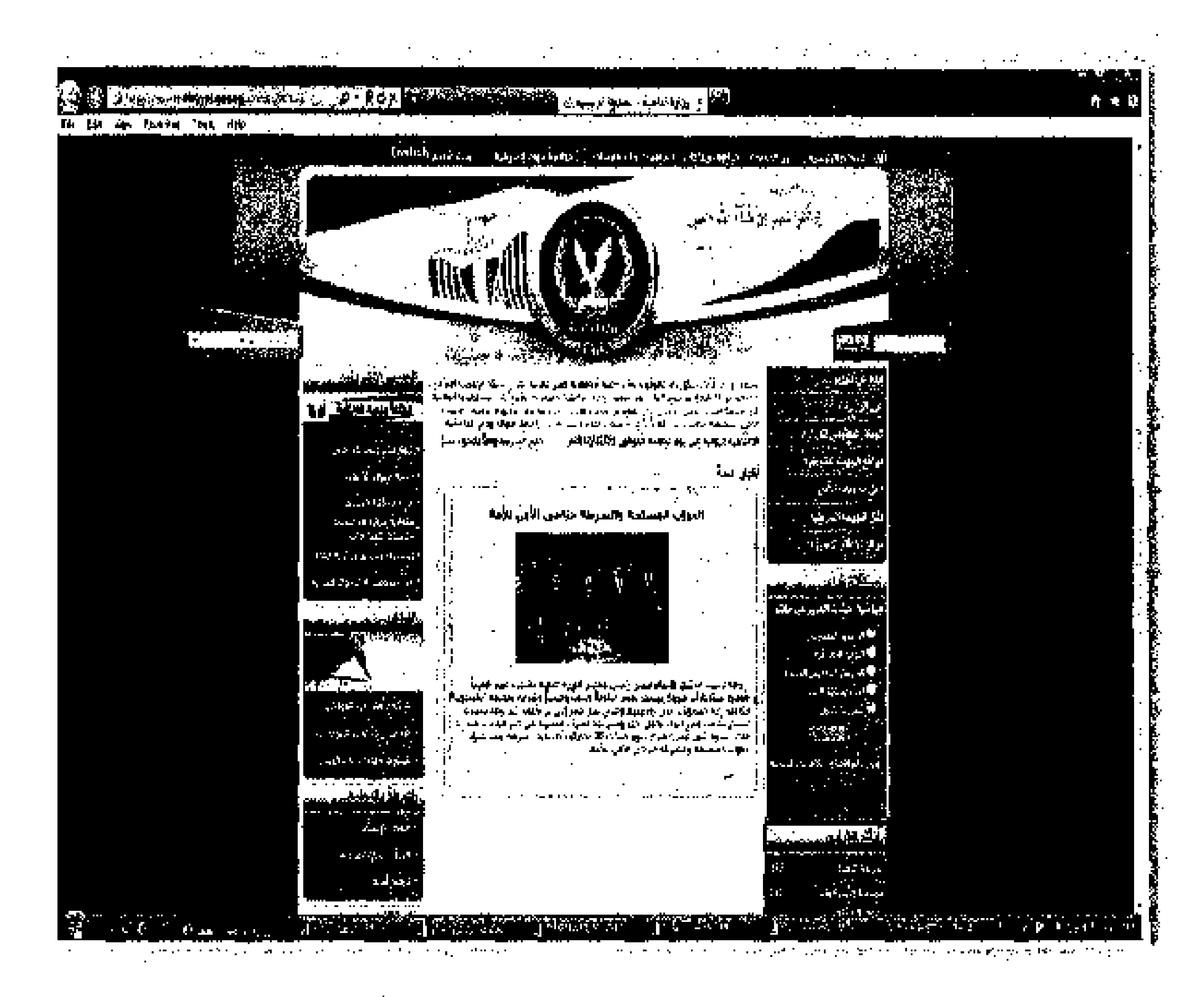
- سهولة الوصول للخدمات إلكترونية من خلال النشر الإلكترونى وهذا يحقق مبدأ الشفافية والعدالة لكافة شرائح المجتمع وتعزيز الديمقراطية، والعمل على تحسين الخدمات من خلال التعرف على أهم معوقات الخدمات وكيفية مواجهتها وتطويرها ويحقق ذلك للمنتفعين مقدار من الثقة والثبات.

ثانيًا - مشروعات وزارة الداخلية المصرية فى مجال الحكومة الإلكترونية:

قامت وزارة الداخلية بالعديد من المشروعات والتطبيقات لتنفيذ نظام الحكومة الإلكترونية متمثلة فى محورين رئيسيين وأحدهما متاح للكافة الاطلاع عليه ويتم تقديم الخدمات الجماهيرية من خلال شبكة الإنترنت؛ حيث تم إنشاء موقع خاص بوزارة الداخلية بالإضافة إلى المشاركة على بوابة الحكومة الإلكترونية وموقع خاص بمصلحة الأحوال المدنية، والمحور الثانى خاص بالعاملين بوزارة الداخلية فى حدود اختصاص كل فرد يمكن مشاهدة التطبيق المسموح له بالإطلاع عليه ومن خلال شبكة معلومات خاصة بوزارة الداخلية تسمى بالإنترانت يتم تنفيذ العديد من التطبيقات الأمنية من خلالها وتحتوى على معلومات أمنية.

١- إنشاء موقع وزارة الداخلية على شبكة المعلومات الدولية (الإنترنت):

سعت وزارة الداخلية المصرية انطلاقًا من مسئوليتها الوطنية في خدمة قضايا العمل الأمنى إلى تطوير وتحديث فعاليات أداء مختلف الأجهزة الأمنية، وتم افتتاح موقع وزارة الداخلية على الشبكة الدولية للمعلومات (الإنترنت) بتاريخ ٢٤ يناير ٢٠٠٧ ليكون بمثابة التواصل بين المواطنين ووزارة الداخلية، وسوف نتناولها فيما بعد بالتفصيل المناسب.



شكل رقم (١-٤) يوضح الصفحة الرئيسية لموقع وزارة الداخلية على الإنترنت

٢- المشاركة فى بوابة الحكومة الإلكترونية :

تقوم هذه الخدمة بمساعدة المواطنين الذين يرغبون فى الحصول على خدمة حكومية معينة من خلال ملء الاستمارات الخاصة بهذه الخدمة والتى يمكن بسهولة تحميلها من الصفحة نفسها ومن ثَمَّ معرفة أقرب جهة يمكن للمواطن الذهاب والتقدم لها بهذا الطلب من خلال إدخال اسم الجهة مقدمة الخدمة والمحافظة ومن ثَمَّ الحى أو المدينة التى يتواجد بها المواطن وبذلك يتم إظهار أقرب جهة مقدمة للخدمة المطلوبة بكافة التفاصيل كالعنوان ورقم التليفون.

يقوم قطاع مصلحة الأحوال المدنية بمختلف الخدمات الخاصة بأوجه الحالة المدنية للمواطن المصرى من حيث الميلاد والزواج والطلاق والوفاة وتسجيلها وإصدار الوثائق والمستندات الدالة عليها داخل وخارج البلاد، كما تقدم الإدارة العامة لشرطة السياحة والآثار خدمة تقديم الشكاوى للسائحين.



شكل رقم (٢-٤) يوضح الصفحة البريد الإلكترونى على شبكة الإنترانت

٣- شبكة المعلومات الداخلية لوزارة الداخلية (الإنترانت) :

تعد شبكة معلومات وزارة الداخلية (الإنترانت) هى التى تُتيح انسياب المعلومات وتبادلها بين قطاعات الوزارة بأسلوب تقنى مُتطور، فى إطار من السرية وعدم القُدرة على اختراقها من خارج الوزارة، وقد استخدم فى بناء البنية الأساسية للشبكة تقنية الإنترنت نفسها ؛ فى شكل شبكة خاصة مغلقة، تتكون البنية الأساسية لها من مجموعة من الحواسب الكبيرة (الخادمة) التى ترتبط ببعضها عبر شبكات مغلقة، وخطوط لنقل المعلومات، وأنظمة للتأمين على مستويين العام والخاص؛ حيث تم تزويد بعض الجهات المتعاملة مع الشبكة بأجهزة حاسبات كبيرة مرتبطة مع المركز الرئيسى للشبكة لبث معلوماتها والبيانات المهمة من خلال البرامج التى تم بناؤها لتحقيق هذا الغرض، والاستفادة منها فى التغلب على المعوقات الزمنية والنمطية، بما يُتيح إمكانية اتخاذ القرار السليم، بناءً على قاعدة معلومات أمنية مؤمنة، وقد تم دعم جميع جهات الوزارة بأجهزة حاسبات آلية لربطها بقاعدة البيانات المركزية، للاستفادة منها فى القيام بالواجبات والمهام، وتطوير نُظم العمل بقطاعات الوزارة المنوط بها تأدية خدمات جماهيرية، لتيسير وتبسيط الإجراءات على المواطنين، وهى تتكون من مركز الحاسبات بالإدارة العامة للمعلومات والتوثيق مرتبط بمجموعة من مراكز المعلومات للإدارات التخصصية، إضافة إلى شبكة معلومات استراتيجية مرتبطة بمراكز معلومات فرعية تغطى جميع القطاعات النوعية و الجغرافية، والمنافذ البحرية والجوية والبرية على مستوى الجمهورية، كما ترتبط بوحدات معلومات فى مراكز أقسام الشرطة، إدارات المرور، إدارات شرطة النجدة، وجميع جهات الوزارة المختلفة، وسوف نتناولها فيما بعد بالتفصيل المناسب.



شكل رقم (٤-٣) يوضح الصفحة الرئيسية لشبكة الإنترانت لوزارة الداخلية



شكل رقم (٤-٤) يوضح الصفحة البريد الإلكترونى على شبكة الإنترانت



٤- تطبيق نظام البريد الإلكتروني :

يتطلب العمل الأمني تبادل كم هائل من المكاتبات التي كان يستخدم في تبادلها الوسائل التقليدية تماشيًا مع نظم الإدارة التقليدية التي كانت تتبع فيما قبل، ومع تطور العمل الأمني واستخدام التكنولوجيا كأحد مفردات الاستراتيجية الأمنية، مع الاعتماد على الإدارة الإلكترونية واستخدام التقنية الرقمية تم استبدال الوسائل التقليدية في تبادل المكاتبات بالوسائل الإلكترونية الرقمية وذلك باستخدام البريد الإلكتروني الآمن على شبكة الإنترانت، لتداول المكاتبات بين الجهات الأمنية المختلفة .

من خلال تحميل هذه الخدمة على شبكة المعلومات المُغلقة للوزارة (الإنترانت)، والمُمتدة جغرافيًا إلى جهات الوزارة المعنية، لسرعة تبادل المُراسلات في سرية تامة، واختصار الوقت، وإرسال حجم كبير من الرسائل مُتعددة الوسائط، وإمكانية إرسال المُكاتبات لأكثر من جهة في الوقت نفسه.

وظائف ومقومات البريد الإلكتروني :

- تبادل الملفات والمعلومات والتوجيهات إلكترونيًا عبر الشبكة؛ حيث يساعد ذلك في تقديم الدعم الفني للجهات المختلفة.
- إرسال رسالة بريدية إلى جهة أو جهات متعددة في اللحظة ذاتها .
- استخدام تطبيقات البريد الإلكتروني بشكل واسع على مستوى جميع جهات الوزارة وإلغاء التعامل مع البريد العادي.
- خاصية إشعار التراسل بتاريخ وساعة فتح المرسل إليه الرسالة البريدية وفي حالة إرسال رسالة بريدية إلى أكثر من جهة يقوم التطبيق بأشعار المرسل ببيان تفصيلي بالجهات التي تسلمت الرسالة والجهات التي لم تستلمها بعد وذلك من خلال النقر على موضوع الرسالة.

٥- مراكز معلومات بقطاعات الوزارة:

تم إنشاء أكثر من مائة وعشرين (١٢٠) مركز معلومات بمُختلف قطاعات الوزارة، وتزويدها بأجهزة حاسبات آلية، تم ربطها بشبكة المعلومات الرئيسية، بُغية بناء قواعد البيانات التى تُحقق الدعم المعلوماتى للقيادات الإشرافية وأجهزة المُكافحة، بما يُسهم فى تعزيز قُدرتها على وضع خطط التأمين والضبط، واتخاذ القرار المبنى على أُسس علمية.

٦- شبكة التراسل الخاصة بالوزارة (Multi - Service Private Network) :

استهدفت خطة وزارة الداخلية مواكبة التقدم التطور العلمى والتكنولوجى، ارتكزت على تنفيذ الشبكة استراتيجية ليمكن تحقيق الاتصال السريع من خلال شبكة خاصة مؤمنة لربط الاتصالات السلكية واللاسلكية والنقل والتبادل الفعَّال للبيانات والمعلومات بدرجة عالية الكفاءة بين مختلف الإدارات والمصالح فى الوزارة، وتحقيق السيطرة الأمنية، ودعم وتعزيز وجود قاعدة بيانات ضخمة، يكون فيها بين مختلف الإدارات والمصالح، وهو حجر الزاوية الأساسى بما ينعكس آثاره على كفاءة الأداء، والمساعدة فى اتخاذ القرار بالدقة المطلوبة وفى التوقيت المناسب، وهذه الشبكة المعروفة باسم التراسل قامت بتنفيذها الإدارة العامة للاتصالات بوزارة الداخلية، باستخدام تكنولوجيا الألياف الضوئية، من خلال وسط تراسلي خاصة (STMI)، وتم توفيره خصيصًا لوزارة الداخلية، لربط جميع مديريات الأمن وإدارات شرطة النجدة ومحطات اللاسلكي بشبكة وزارة الداخلية، ولديها القدرة على تغطية كافة الأرجاء، وهو ما دفع الجهاز الأمنى لتنفيذها وارتباطها بجميع مديريات الأمن، بالإضافة إلى كونها شبكة خاصة يضيف عنصر التأمين لتداول البيانات والمعلومات على الشبكة لصعوبة الاختراق من الخارج.

٧- شبكة نقل المؤتمرات المرئية (Video Conference System) :

إن شبكة التراسل الاستراتيجية الخاصة بوزارة الداخلية تتيح عقد مؤتمرات مرئية مباشرة بين وزير الداخلية، مع أكثر من قيادة أمنية فى وقت واحد،وذلك من خلال وحدات المؤتمرات المرئية التي تستخدمها الشبكة المنفذة، مما يساعد على تبادل الآراء ومناقشة الخطط الأمنية ومراجعتها، ويُمكن أيضا من خلالها تنظيم مؤتمرات واجتماعات ولقاءات مرئية عن بُعد، لمختلف المستويات القيادية والإشرافية بالوزارة، دون حاجة للانتقال، بما يُتيح سرعة تلقى البيانات والمعلومات، وترشيد اتخاذ القرار.

٨- شبكة نقل الأحداث المرئية (Video active vransmies network) :

شبكة التراسل الاستراتيجية يُمكن من خلالها نقل ومُتابعة الأحداث من موقعها ولحظة حدوثها إلى جميع المُستويات القيادية فى الوقت نفسه، بما يُمكنها من سرعة تبادل ومتابعة البيانات والمعلومات عن الحدث واتخاذ القرار المُناسب، مما يحقق الاتصال المباشر بين متخذ القرار، والقوات أثناء العمليات فى أي موقع داخل مصر، مع ربط السنترالات الخاصة بوزارة الداخلية بشكلٍ موحد، وهو ما يتيح الاتصال والترابط بين مديريات الأمن وأية نقطة وموقع شرطي فى المحافظات الـ٢٧، كما يتيح هذا المشروع نقل وتبادل المعلومات واستخدام قواعد البيانات عن طريق دعم ونشر شبكات نقل المعلومات الحالية، وتفعيل مفهوم استخدامها كقاعدة بيانات وتبادلها فى حدود المسموح بين هذه المصالح وبعضها البعض وبين فروعها، مما سيكون له مردود أمني واسع من حيث سرعة تلقي المعلومة، وتوفير هائل للجهد المبذول يعود على ديناميكية الحركة داخل قطاعات الوزارة وسرعة التصرف واتخاذ القرار.

٩- مشروع الخدمة الصوتية للخدمات الأمنية الجماهيرية :

إن الخدمات الجماهيرية المباشرة كان لها اهتمامها الخاص من جانب وزارة الداخلية

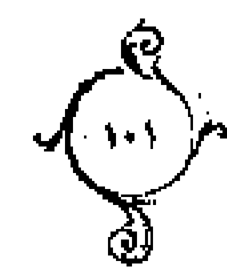


ومنها خدمة الرسائل الصوتية، التي استُحدثت خصيصًا لهذا الهدف؛ حيث يقوم المواطنون بالاتصال برقم(١٢٨) من أى تليفون محمول أو عادى للدخول على الخدمة الصوتية لوزارة الداخلية للاستعلام عن الخدمات الجماهيرية التى تقدمها الوزارة للمواطنين، ومن خلالها التعرف على كافة التفاصيل والمعلومات المطلوبة للحصول على الخدمات الأمنية الجماهيرية (المرور- الأحوال المدنية - الجوازات - تصاريح العمل- الأدلة الجنائية ... إلخ)، ليتعرف المواطن على جميع المستندات المطلوبة فى الإدارات والمصالح المختلفة، ونظرًا للإقبال الجماهيرى على هذه الخدمة؛ فقد تمت زيادة عدد الخطوط من (٣٠) خط إلى (٩٠) خط.

ثالثًا- تكنولوجيا المعلومات الأمنية فى مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية :

يعيش العالم الآن عصر «ثورة المعلومات»، والتى ترتبط ارتباطًا وثيقًا بتكنولوجيا عصر المعلومات، وأصبحت المعرفة هى محور التقدم، وتعد الشعوب المتخلفة هى تلك التى لم تدخل ثورة المعلومات حتى اليوم، فالمعلومات هى القوة التى تحفظ للشعوب استقلالها، وتعتبر المعلومات قوة حضارية، ضرورية لتطور الشعوب وتقدمها، كما أن النمو الاقتصادى يرتبط ارتباطًا طرديًا بكمية المعلومات، ونوعيتها، والطريقة التى يتم الإلمام بها، وتطبيق ما جاء فيها.

واهتمت الحكومة المصرية بتكنولوجيا المعلومات من خلال تطوير أسلوب العمل بنظام الحكومة الإلكترونية من أجل تحقيق أهداف البرنامج كان من الضرورى توفير قنوات مختلفة ومتنوعة لتوصيل الخدمات إلى المواطن بالأسلوب الذي يناسبه، سواء كان ذلك من خلال الإنترنت أو التليفون أو منافذ مختلفة منتشرة على مستوى الجمهورية؛ حيث يقوم المواطن بطلب الخدمة وتقوم الهيئة القومية للبريد بتوصيلها إليه فى المكان الذى يحدده.



بوابة الحكومة المصرية[1] :

منذ إطلاق بوابة الحكومة المصرية رسميًا عام ٢٠٠٤، يتم إتاحة العديد من الخدمات الحكومية من خلالها، وكذلك ربطها بالمواقع الإلكترونية لمختلف الجهات الحكومية والمحافظات، ويهدف البرنامج إلى إضافة خصائص جديدة للبوابة مثل إتاحة خاصية التوقيع الإلكترونى، وذلك بهدف ضمان استمرارية تشغيلها بكفاءة وفعالية، وتحقيق رضاء أكبر عدد من المستخدمين من مواطنين وأجانب، وتلبية للطلب المتنامى على الخدمات الحكومية الإلكترونية.

مراكز اتصال الحكومة المصرية ١٩٤٦٨ :

يعد تقديم الخدمات الصوتية للجماهيرية من خلال مركز الاتصال ١٩٤٦٨ والذى يربط حتى الآن ما يزيد على خدمات أربعون (٤٠) جهة حكومية، بالإضافة إلى مراكز اتصال لدى الجهات التى تقدم بعض الخدمات الحكومية المستقلة مثل ١٩٩٨٤، وخدمات وزارة الداخلية من خلال الرقم (١٢٨).

منافذ تقديم الخدمات الجماهيرية :

وتوفر منافذ تقديم الخدمات الجماهيرية خدماتها للمواطنين؛ حيث يتقدم إليها المواطن بالمستندات المطلوبة، يقوم مقدم الخدمة بالتعامل مع الجهة الحكومية المختصة للحصول على الوثائق المطلوبة ثم إتمام الخدمة بتسليمها للمواطن، وهنالك العديد من المواقع المرتبطة ببوابة الحكومة الإلكترونية، ويعد موقع بوابة وزارة الداخلية من أهم المواقع المرتبطة بها.

---

(1) www.egypt.gov.eg



موقع وزارة الداخلية على شبكة المعلومات الدولية (الإنترنت) :

تم افتتاح موقع وزارة الداخلية على الشبكة الدولية للمعلومات (الإنترنت) بتاريخ ٢٤ يناير٢٠٠٧م ليكون بمثابة التواصل بين المواطنين ووزارة الداخلية، وانطلاقًا من المسئولية الوطنية فى خدمة قضايا العمل الأمني وتقديم الخدمات الجماهيرية عبر موقع الوزارة، ودعمًا لعجلة التنمية والاستثمار فى مختلف المجالات، وحث رجال الشرطة على الاستمرار والتطوير المستمر لما يحقق خدمه المواطنين، وتماشيًا مع سياسية الدولة لتحقيق الحكومة الإلكترونية.

ويتضمن هذا الموقع محورين رئيسيين، وهما:

أ- المحور الإعلامي :

يتمثل المحور الإعلامى فى تعريف وزارة الداخلية فى المراحل التاريخية وفى أحقاب زمنية مختلفة، وكذا التعرف على الهيكل التنظيمى للوزارة بالإضافة إلى عرض الأخبار والأحداث المهمة التى تهم المواطن وإعطاء فكرة عن أنشطة القطاعات المختلفة داخل الوزارة.

ب- المحور الخدمي:

يتمثل المحور الخدمى فى تقديم تلك الخدمات التي تقدمها الوزارة للمواطنين والإرشادات المرتبطة بها بالإضافة إلى بعض الأمور التى تهم المواطن وكذا البلاغات والشكاوى، وفيما يلى سوف نعرض صفحات الجهات الشرطية داخل موقع وزارة الداخلية على شبكة الإنترنت.

شكل رقم (٥-٤) يوضح مواقع الجهات الشرطية[1]

(1) www.egypt.gov.eg



١- الإدارة العامة للإعلام والعلاقات :

يتم من خلال الصفحة الإلكترونية للإدارة العامة للإعلام والعلاقات الإعلام عن نشاطات الوزارة والأخبار الصادرة عن المركز الإعلامى وأهم البيانات الصادرة عن الوزارة للرد على ما يثار خارجيًا وداخليًا حول القضايا الأمنية فى مصر وكذا المؤتمرات والندوات التى تعقدها الوزارة، بالإضافة إلى التعريف بمركز الإعلام الأمني من حيث النشأة والأهداف وبث البيانات الأمنية، والموجز اليومى، وعرض لأهم القضايا، ومتابعة ما تبثه وكالات الأنباء العالمية وشبكة الإنترنت وتصنيفه وأرشفته وتخزينه مع إمكانية استدعائه، وإعداد تقرير يتضمن أهم الأخبار، وبثهما على شبكة معلومات الوزارة لتتاح فرصة وصول الأخبار المهمة لحظيًا إلى الجميع، والاهتمام بتغطية الأنشطة التي يقوم بها السيد الوزير وتوثيقها وأرشفتها، بالإضافة لوجود رابط للاتصال بالإدارة.



شكل رقم (٦-٤) يوضح موقع الإدارة العامة للإعلام والعلاقات



٢- أكاديمية الشرطة :

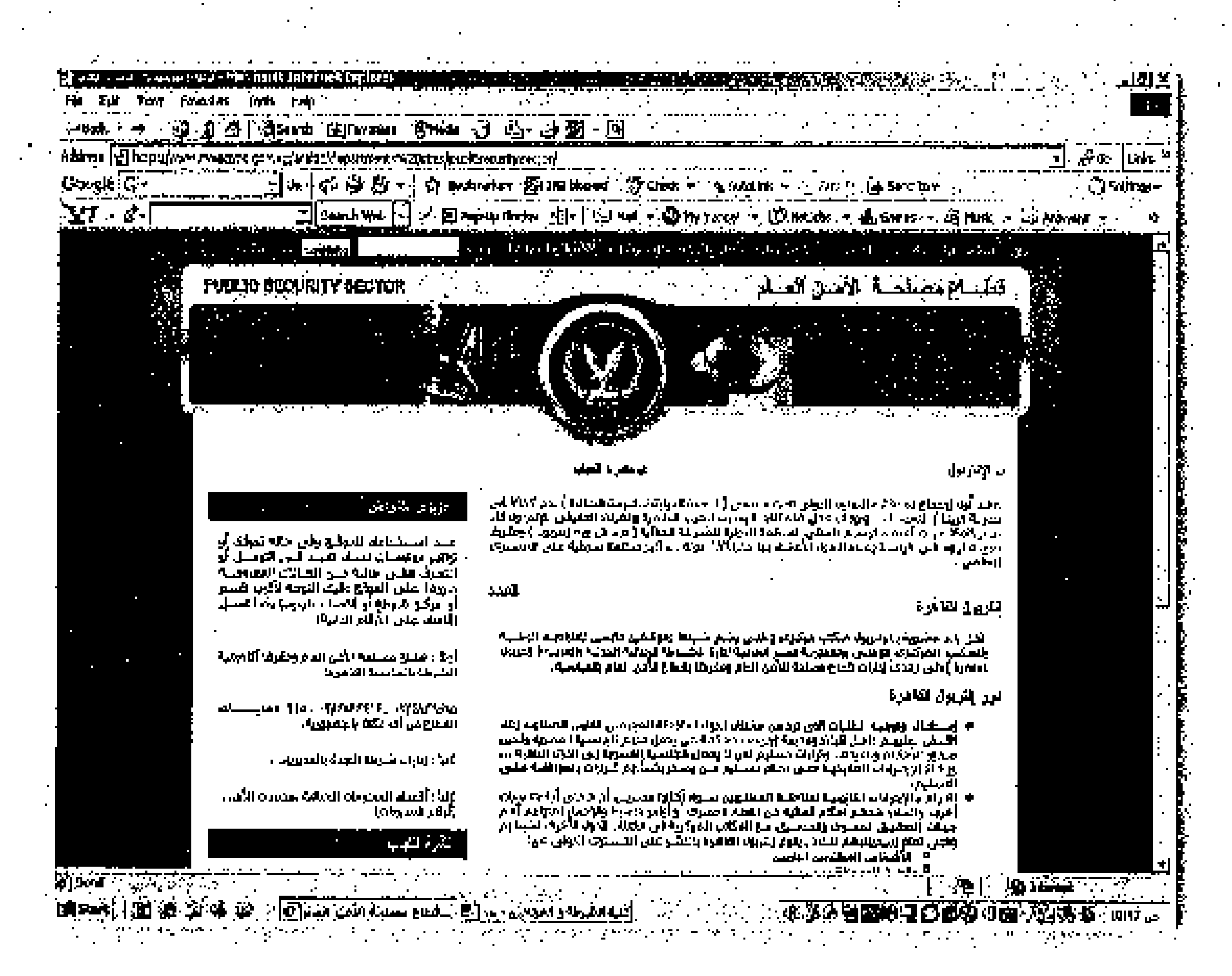
تحتوي هذه الصفحة على عرضًا كاملاً عن أكاديمية الشرطة وأهدافها والكليات التابعة لها وأهم الأنشطة وشروط الالتحاق وخطة الدراسة بكلية الشرطة، كما يتم بث آخر أبحاث مركز بحوث الشرطة والندوات والمؤتمرات التي ينظمها، كما تتيح تلك الصفحة الدخول على تطبيق التقديم كلية الشرطة ويتم من خلاله تسجيل بيانات الطلبة المتقدمين للاختبارات، وعرض نتائج كافة الاختبارات للطلبة المتقدمين من خلال شبكة معلومات الوزارة.



شكل رقم (٧-٤) يوضح موقع أكاديمية الشرطة

٣- قطاع مصلحة الأمن العام :

تعرض صفحة مصلحة الأمن العام موجز عن الإنتربول وتعريف عن إدارة الشرطة الجنائية الدولية العربية (انتربول القاهرة) ودورها في مجال مكافحة الجريمة، وفي إطار اهتمام وزارة الداخلية بمجالات الغياب والجثث المجهولة والضالين وفاقدي الذاكرة والمصابين والمرضى المجهولين، تضمنت صفحة مصلحة الأمن العام عرض للغائبين لإتاحة الفرصة لمستخدمي شبكة الإنترنت الاطلاع على البيانات والمعلومات والصور الخاصة بتلك الحالات للمساهمة في الاستدلال عليهم، والاهتداء لأسرهم من خلال إتباع الإجراءات الموضحة بالموقع.



شكل رقم (٨-٤) يوضح موقع قطاع مصلحة الأمن العام.



٤- مصلحة الجوازات والهجرة والجنسية:

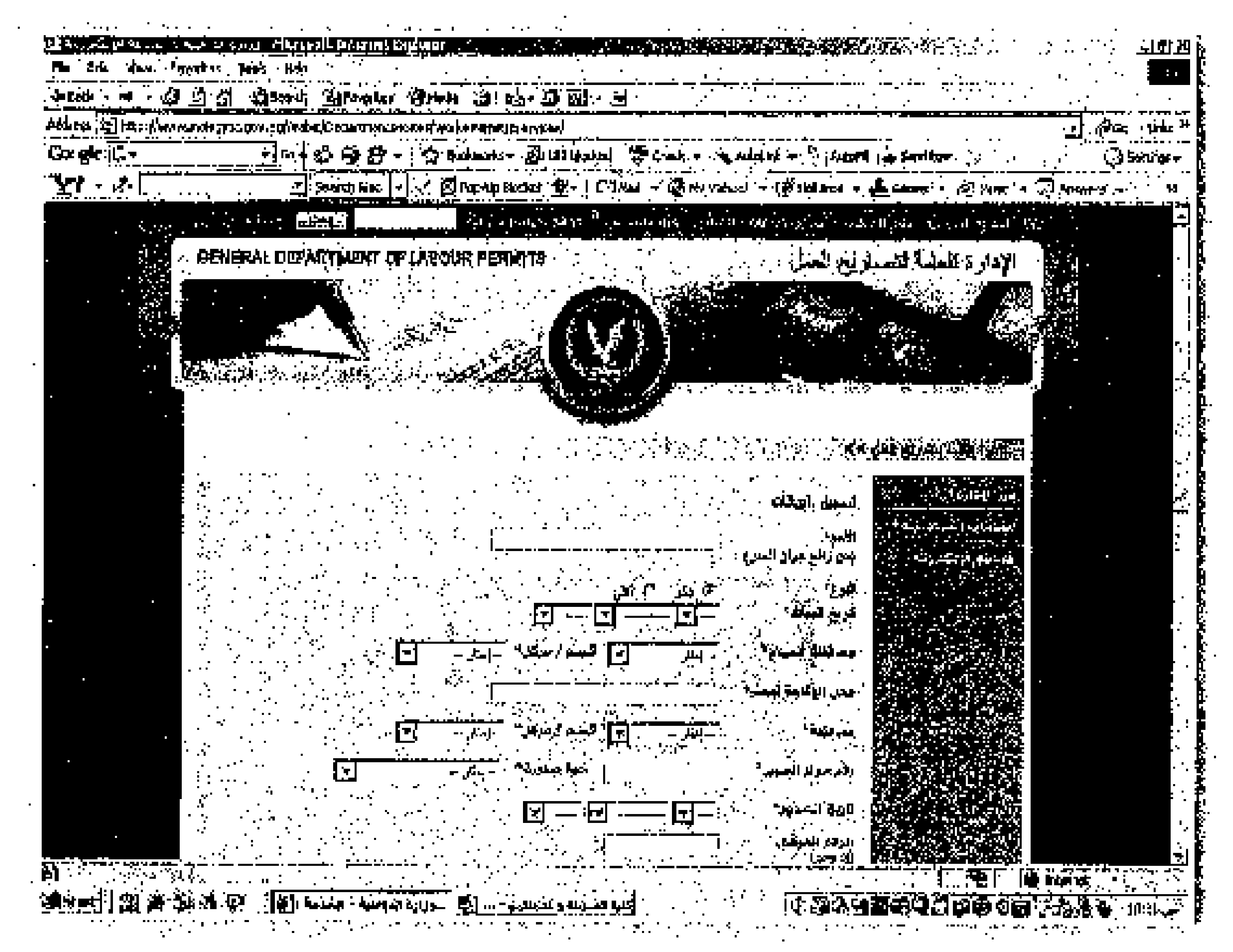
تتضمن صفحة مصلحة الجوازات والهجرة والجنسية، عرض وتصنيف الإجراءات المتعلقة بإصدار وثائق السفر، ومنح تصاريح الإقامة، وحركة المسافرين والداخلين عبر المنافذ الشرعية للبلاد، والإجراءات الخاصة بالهجرة والجنسية، وإقامة الأجانب، وكافة الخدمات التى تقدمها المصلحة من وثائق السفر وطلبات الهجرة والجنسية وشهادات التحركات وتنفيذ الأحكام القضائية بالإضافة إلى قواعد سفر المواطنين للخارج، بهدف تطوير وتبسيط إجراءات الجنسية، والهجرة، والإقامة، وإجراءات إصدار وثائق السفر، ودقة وسرعة الحصول على البيانات المتعلقة بحركة السفروالوصول للمواطنين والأجانب، كما تضمنت الصفحة نبذة تاريخية عن المصلحة، والإجراءات المطلوبة لإصدار وثائق السفر، وقواعد سفر المواطنين للخارج، ونموذج طلب الشهادات للجهات القضائية، وطلبات تنفيذ الأوامر الوقتية والأحكام القضائية، وقسم البلاغات، وتعريف بأقسام الجوازات والمنافذ البرية والبحرية والجوية على مستوى الجمهورية.



شكل رقم (٤-٩) يوضح موقع مصلحة الجوازات والهجرة والجنسية

٥ - الإدارة العامة لتصاريح العمل :

تضمن هذه الصفحة دور الإدارة فى المجالات المختلفة الأمنية والاقتصادية والخدمات الجماهيرية التى تقدمها، وشروط وإجراءات حصول المواطن عليها وتيسير استخراج تصريح العمل، كما تضمن نموذجًا يمكن للمواطنين الراغبين فى تجديد تصاريح العمل الخاصة بهم، وبهدف إصدار تصاريح العمل وفقًا للقواعد، وتبسيط إجراءات إصدارها وتجديدها، ويتم التعامل مع هذا النموذج وإرسال البيانات المطلوبة ودفع الرسوم إلكترونيًا عبر الإنترنت للإدارة العامة لتصاريح العمل لتجديد التصريح المطلوب، ويخدم ذلك عددًا كبيرًا من العاملين فى الخارج وييسر تقديم الخدمة لهم.



شكل رقم (١٠-٤) يوضح موقع الإدارة العامة لتصاريح العمل



٦- الإدارة العامة للشئون الإدارية :

تتضمن الصفحة الإلكترونية للإدارة العامة للشئون الإدارية خدمات الإدارة فى مجال الحج والعمرة، المتعلقة بشروط وقواعد وإجراءات الحج والعمرة، لتبسيط وتيسير إجراءات المواطنين للحج والعمرة، ودقة المعلومات والبيانات، ومتابعة إجراءات السفر للحج والعمرة طبقًا للقواعد المقررة، والإرشادات العامة للحجاج المصريين تعد من الأمور المهمة التى تحرص عليها الوزارة، والعمل على خلق الارتباط والتواصل بين الوطن وحجاج بيت الله الحرام بالأراضى السعودية فى مواسم الحج، وبث الأخبار المهمة والتيسيرات التى تقدمها فى هذا المجال، وأيضًا التصديق على الشهادات وتتعرض لضوابط تعيين العمد والمشايخ.



شكل رقم (١١-٤) يوضح موقع الإدارة العامة للشئون الإدارية

٧- الإدارة العامة للمرور :

تعرض هذه الصفحة أهم الأخبار المرتبطة بالمرور والتى تهم المواطن بالإضافة إلى قواعد وآداب المرور والجديد فى هذا المجال وخدمات المرور والعقوبات المرتبطة به عن طريق ميكنة جميع البيانات الخاصة بالمركبات ورخص القيادة والحوادث والمخالفات المرورية، بُغية تبسيط الإجراءات الخاصة باستخراج رخص القيادة ورخص تسيير المركبات، وشهادة البيانات، وتلبية الاحتياجات الأمنية من معلومات عن المركبات ورخص القيادة بدقة فائقة، وإصدار تراخيص مُميكنة وغير قابلة للتزوير.

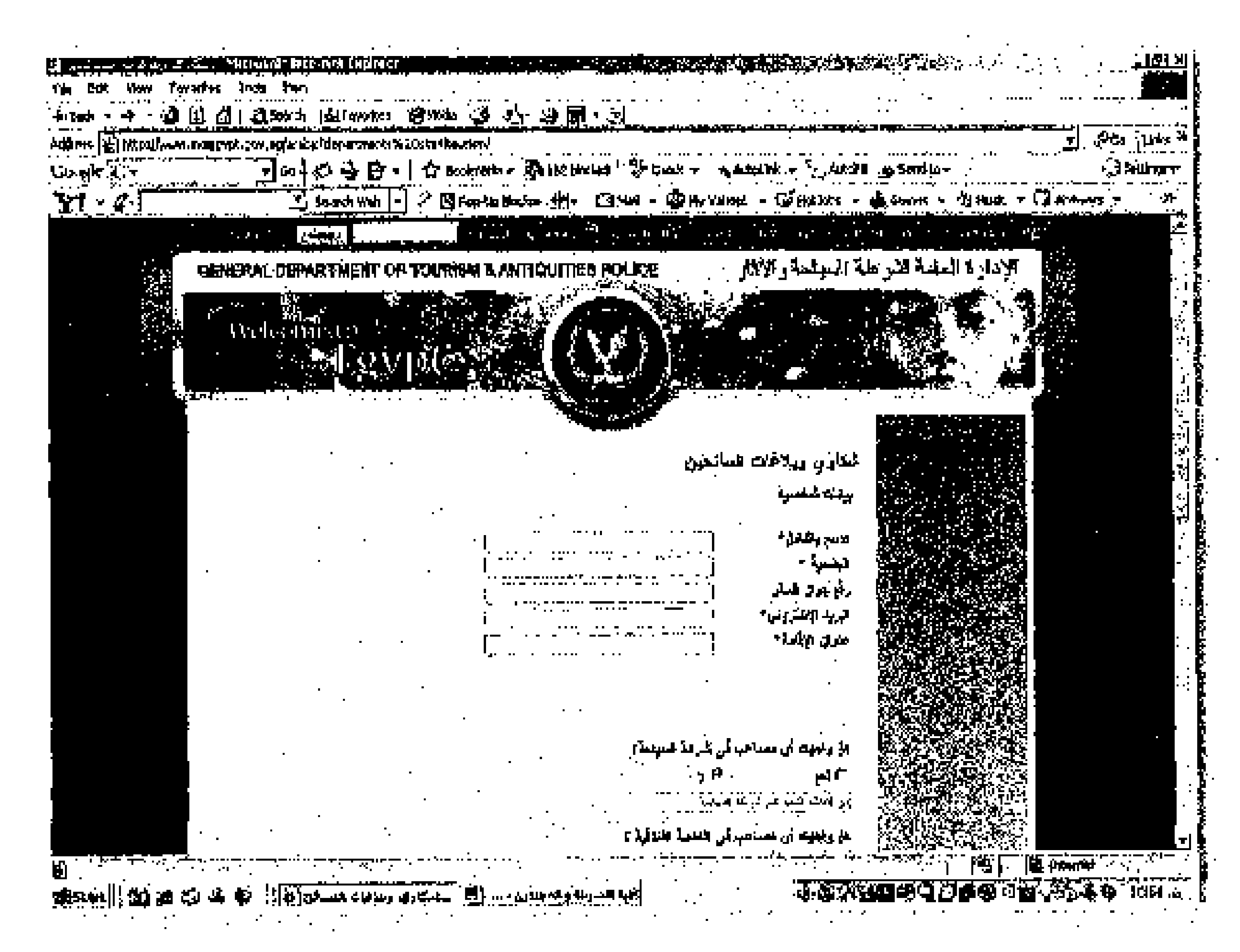


شكل رقم (١٢-٤) يوضح موقع الإدارة العامة للمرور



٨- الإدارة العامة لشرطة السياحة والآثار :

تعد هذه الصفحة لتلقى البلاغات و الشكاوى من السائحين من الأمور المهمة لمواجهه لأية صور استغلال أو لدراسة المصاعب التى تواجه السائحين فى مجالات التعامل اليدوى، مما يعد مصدرًا مهمًا لمواجهة صور الإساءة أو الاستغلال المختلفة أو لتصحيح الأمور التى تُشكل مصاعب أو مشاكل للسائحين وذلك بهدف الوصول إلى أفضل مستوى من الخدمة الأمنية لزائرى جمهورية مصر العربية من الاطمئنان والراحة ودعمًا للتنمية والاستثمار فى مجال السياحة.



شكل رقم (١٣-٤) يوضح موقع الإدارة العامة للشرطة السياحة والآثار

٩- قطاع مصلحة السجون :

دعمًا لحقوق الإنسان فإن صفحة مصلحة السجون تتعرض لأهم أوجه الرعاية الاجتماعية والصحية للسجناء بالإضافة إلى نبذة عن قطاع مصلحة السجون وتطور السياسة العقابية فى السجون المصرية وتأهيل السجناء وتوفير فرص العمل لهم، كما تتضمن الصفحة تعريفًا للخدمات الجماهيرية التى تقدمها المصلحة للمواطنين القادمين لزيارة ذويهم سواء كانت الزيارة عادية أو خاصة وكيفية صرف المساعدة المالية أو المعاش لأسر المسجونين.



شكل رقم (١٤-٤) يوضح موقع قطاع مصلحة السجون

١٠- الإدارة العامة لمكافحة المخدرات :

تهدف هذه الصفحة إلى نشر الوعى لدى الجمهور إلى الآثار الضارة للمخدرات ونشر تعريف عن الإدارة العامة لمكافحة المخدرات، والأجهزة الوطنية للمكافحة، وعرض للتقرير السنوى، والتدريب فى مجال المكافحة، والتطور التشريعى فى هذا المجال، وعرض لأهم أنواع المخدرات، والآثار الضارة للمخدرات، وتتناول طرق التوعية، وأهم القضايا والآثار الاجتماعية والصحية والاقتصادية الأمنية وعرض لمكتبة الإدارة، ومتحف الإدارة، وفى النهاية البلاغات، مما يساهم فى زيادة الوعى لأخطار المخدرات.



شكل رقم (١٥-٤) يوضح موقع الإدارة العامة لمكافحة المخدرات

١١ - الإدارة العامة لمكافحة جرائم الأموال العامة :

تهتم صفحة الأموال العامة بنشر الوعي لدى الجمهور في مجال الجرائم المرتبطة بالأموال العامة من خلال نشر العلامات ووسائل التأمين الخاصة بالعملات الوطنية والأجنبية، وأهم الإرشادات في التفرقة بين العملات الوطنية والأجنبية الصحيحة والمقلدة، ومعلومات عن مخاطر الهجرة غير المشروعة، وعن خطورة ظاهرة الرشوة وتأثيراتها السلبية على الوظيفة العامة، مع عرض جانب من الجرائم التي تم ضبطها، وبعض التوجيهات لتجنب الوقوع ضحية للنصب والاحتيال وجرائم غسل الأموال وسفر العمالة المصرية للخارج، ليكون لدى المواطن دراية بهذه الأمور وتجنب الوقوع ضحية لمثل هذه الجرائم وإرسال البلاغات عبر الشبكة للإدارة العامة للأموال العامة لزيادة التفاعل بين المواطن والوزارة في مكافحة هذه الجرائم.



شكل رقم (١٦-٤) يوضح موقع الإدارة العامة لمكافحة جرائم الأموال العامة

١٢ - قطاع مصلحة الأحوال المدنية :

فى إطار سياسة وزارة الداخلية لتقديم كافة التيسيرات للمواطنين للحصول على الخدمات باستخدام تكنولوجيا المعلومات والاتصالات فقد تم تطوير أسلوب تقديم عدد من خدمات قطاع مصلحة الأحوال المدنية متمثلة فى (شهادات الميلاد المميكنة - بطاقات الرقم القومى «بدل فاقد/تالف») لمن سبق لهم استخراج بطاقة الرقم القومى ليتمكن المواطن من الحصول على الوثائق المطلوبة عن طريق البريد السريع باستخدام شبكة المعلومات الدولية على الموقع التالى (www.cso.gov.eg)، ودون حاجة للانتقال إلى مقار المصلحة؛ حيث يقوم المواطن بالدخول على موقع قطاع مصلحة الأحوال المدنية أو الدخول من خلال بوابة الحكومة الإلكترونية واختيار خدمات مصلحة الأحوال المدنية، أو الدخول على موقع وزارة الداخلية واختيار خدمات مصلحة الأحوال المدنية، وملء البيانات الخاصة بالمستند المطلوب ثم سداد قيمة المستندات وتكلفة البريد من خلال بطاقات الائتمان (فيزا،ماستر كارد) يتولى قطاع مصلحة الأحوال المدنية مراجعة البيانات وإصدار الوثائق على أن يتولى البريد السريع توصيل الخدمة للمنازل خلال ٤٨ إلى ٧٢ ساعة، وأيضًا يمكن الاستعلام عن موقف الخدمة فى غضون أسبوع من طلبها فى حالة تأخرها لاحتمال وجود اختلاف فى البيانات المطلوبة عن المسجلة على الحاسب يجب على المواطن التوجه إلى المصلحة أو الإدارات التابعة لها بالمستندات الدالة على البيانات المطلوبة لتصحيحها بالسجلات.

هذا ويحق لقطاع مصلحة الأحوال المدنية رفض تقديم تلك الخدمة عن طريق الإنترنت لغير المستفيدين السابق إيضاحهم ويمكن لطالب الخدمة التوجه إلى أحد أفرع المصلحة للاستفسار.

وفيما يلي قائمة بالخدمات التي تقدمها مصلحة الأحوال المدنية مقسمة طبقًا لنوعياتهم:

وقائع الميلاد :

استخراج شهادة الميلاد أول مرة، استخراج صورة قيد شهادة ميلاد لأول مرة مميكنة، استخراج صورة قيد شهادة ميلاد للقنصليات بالخارج، فحص طلب قيد ساقط الميلاد إذا تقدم بالطلب قبل مرور عام من تاريخ الميلاد، فحص طلب قيد ساقط الميلاد إذا تقدم بالطلب بعد مرور عام من تاريخ الميلاد.

وقائع الزواج والطلاق :

استخراج صورة قيد الزواج المميكنة، استخراج صورة قيد الطلاق المميكنة، وقائع الوفاة، استخراج شهادة الوفاة أول مرة، استخراج صورة قيد شهادة وفاة مميكنة، فحص طلب قيد ساقط الوفاة إذا تقدم بالطلب قبل مرور عام من تاريخ الوفاة، فحص طلب قيد ساقط الوفاة إذا تقدم بالطلب بعد مرور عام من تاريخ الوفاة.

إصدار بطاقة الرقم القومي و القيد العائلي المميكن :

إصدار بطاقة الرقم القومي (أول مرة،بدل فاقد،بدل تالف،تغيير بيانات،إعادة تصوير) مستخرج القيد العائلي المميكن تغيير، تصحيح قيود الأحوال المدنية تغيير قيود الأحوال المدنية المدونة بالسجلات تصحيح قيود الأحوال المدنية المدونة بالسجلات.

شكل رقم (١٧-٤) يوضح موقع قطاع مصلحة الأحوال المدنية

١٣- مصلحة الأدلة الجنائية :

من خلال حصر وتصنيف وتبويب وميكنة البيانات المُتعلقة بإجراءات إصدار صحف الحالة الجنائية، بُغية تبسيط وتيسير إجراءات إصدار صحف الحالة الجنائية وعدم تزويرها، وقد تم استحداث صحيفة الحالة الجنائية المُتكررة (بدون بصمات)؛ حيث يُمكن للأشخاص حاملي بطاقات الرقم القومي استخراج هذه الصحيفة بدون أخذ البصمات مرة أُخرى، في حالة أخذها مسبقًا، وأيضًا المستندات والأوراق اللازمة للحصول على خدمة إصدار نموذج صحيفة الحالة الجنائية، والتصديق على صحيفة الحالة الجنائية.



الفصل الخامس

دور التقنيات الحديثة فى تطوير تكنولوجيا المعلومات الأمنية

الفصل الخامس
دور التقنيات الحديثة فى تطوير تكنولوجيا المعلومات الأمنية

إن التطور التكنولوجى والتقنى الذى يعيشه العالم الآن، جعل التحقق من هوية الأشخاص أمرًا يزداد صعوبة، وقد استلزم هذا التطور الذى يشهده العصر واستفادت منه العناصر الإجرامية فى ارتكاب الجرائم، إلى تطوير وتحديث الإجراءات الأمنية، ويعد استخدام البصمات البيومترية فى التحقق من هوية الأشخاص من خلال صفاته الفسيولوجية أو سماته السلوكية التى يمكن التعرف عليها والتأكد منها آليًا، إحدى الوسائل التى تعتمد عليها الأجهزة الأمنية فى كشف الجرائم ومرتكبيها.

وفى ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتى :

أولاً : مفهوم التقنية البيومترية .

ثانيًا : بصمة الإصبع .

ثالثًا : البصمة الوراثية .

أولاً- مفهوم التقنية البيومترية :

انتشرت التقنية البيومترية بشكل ملموس وسريع في الفترة الماضية، وهي تعد القاعدة الأساسية للتعرف الآمن على الهوية، وتشكل الجزء الأساسي من الأنظمة التي تتطلب تحديدًا دقيقًا للهوية، وكثرت تطبيقاتها في المطارات بشكل خاص، وحولت الكثير من الدول جوازات سفرها وتأشيرات دخولها إلى الشكل البيومتري ليس فقط للمزايا الأمنية التي تتمتع بها، بل أيضًا لما تتمتع به من الملائمة والسهولة في الاستخدام، كذلك كثر استخدام تقنياتها المختلفة للمراقبة، أو كأساس لأنظمة التحكم في دخول أماكن محددة، إلا أن تلك التطبيقات الآن أصبحت منتشرة بشكل كبير حتى وصلت إلى جهاز الكمبيوتر الشخصي لتستخدم كوسيلة لحماية المعلومات.

أصل كلمة «بيومتري» يرجع إلى اللغة اليونانية وينقسم اللفظ إلى جزأين «بيو» وتعني الحياة و«مترية» تعني لأجل القياس، فالتكنولوجيا البيومترية تعتمد على المميزات الخاصة في الجسم، وهي عبارة عن علم يدرس كيفية استخدام معادلات رياضية وإحصائية لقياس العلاقات الرقمية والنسب المختلفة التي تظهر في الكائنات الحية وأعضائها المختلفة، وتسمح بتصوير مصادفات الطبيعة بشكل حسابي وذلك باستغلال كل من نظريات علم الرياضيات وعلم الإحصاء، ويتم التعرف على تلك الصفات عبر جهاز الكمبيوتر الذي يتعرف على بصمات الإصبع عبر المجسات المختلفة مثل الماسح الضوئي لبصمات الأصابع أو ماسح العين والوجه أو قارئ الخطوط الإلكتروني عبر معادلات رياضية دقيقة ومعقدة، يقارن جهاز الكمبيوتر تلك المعلومات بما هو مخزن لديه ليحدد إذا كانت تتطابق معها أم لا ؟[1].

(1) L.C. Jain : Intelligent Biometric Techniques in Fingerprint and Face Recognition, Boca Raton: CRC Press, C1999, p21

وأنواع التقنيات البيومترية كثيرة ومتنوعة، فمنها تقنية التعرف على الوجه أو العينين أو شكل الأذنين إلى التوقيع اليدوى أو طريقة الكتابة على لوحة المفاتيح مرورًا ببصمات الأصابع والشكل الهندسى المميز لليد والحمض النووى المعروف باسم (دى. إن. ايه (DNA)) والتعرف على بصمة الصوت والرائحة المميزة لكل جسد وغيرها من الوسائل المتعددة والمميزة لكل فرد، إلا أن الكثير من تلك التقنيات يعد باهظ الثمن بشكلٍ كبير، ولا يستطيع الكثيرون الاعتماد عليه، لذلك فقد أصبحت تقنية التعرف على بصمة الأصابع الأكثر انتشارًا لأنها الأقل تكلفة، وتتبوأ البصمة مكانة متميزة بين المحددات البيومترية المتنوعة نظرًا لما تتمتع به من مزايا، وقد تم اعتمادها للتعرف على الهوية، وتأمين الدخول والخروج من وإلى المؤسسات. يتكون هذا النظام بشكل أساسى من وحدة معالجة إشارة تقوم باستخلاص السمات المميزة للبصمة والتعرف عليها، ومن حاسب شخصى لإدارة النظام، ومن البرمجيات الخاصة بالتطبيق المذكور للنظام .

لمحة حول الأنظمة البيومترية :

البيومترية تعنى الطرق المؤتمنة للتعرف على الهوية والمعتمدة على المواصفات الفيزيولوجية والسلوكية للشخص المعنى، وتشمل المواصفات الفيزيولوجية أنواعًا عديدة من المحددات مثل البصمة، مقاييس اليد، التعرف على قزحية العين، التعرف على شبكية العين، التعرف على الوجه، كما تشمل المواصفات السلوكية أنواعًا عديدة من المحددات -أيضًا- مثل الصوت، التوقيع، النقر على الملامس(عند الطباعة)، طريقة المشى، التعرف على خط اليد.

تجدر الإشارة إلى أن استخدام الأنظمة البيومترية للتعرف على الهوية ملائم بشكل ملموس؛ (حيث لا يوجد ما يلزم حمله أو تذكره مثل كلمات المرور أو الأرقام أو البطاقات



الشخصية)، وأصبحت هذه الأنظمة مقبولة اجتماعيًا وغير مرتفعة التكلفة.

وانتشار هذه الأنظمة فى نمو مستمر ليس فقط للمزايا الأمنية التي تتمتع بها، إنما أيضًا لما تتمتع بها من الملائمة والسهولة في الاستخدام، وتتكون الأنظمة البيومترية من جزئين هما الكيان الصلب، وهو متمثل فى الأجهزة والأدوات، والكيان اللين، وهو متمثل فى البرمجيات.

وتُشكل عملية التقاط مواصفات المحدد البيومترى مرحلة التسجيل فى النظام البيومترى؛ حيث يتم فيها إدخال البيانات إلى النظام بواسطة الأداة المناسبة (ماسح، كاميرا، ميكرفون ... إلخ)، ثم تقوم برمجيات النظام باستخلاص السمات المناسبة من الشكل الذى تم إدخاله، وتخزين البيانات العائدة له على شكل «قالب»، وعندما يتعامل المستخدم مع النظام البيومترى ثانية فإن النظام يقوم بمقارنة بيانات المستخدم المدخلة مع القالب المخزن مسبقًا عنه، فإن حصل التطابق تم التعرف، وإلا فلا تسمح له، ويمكن إعطاء الحق لأكثر من شخص للدخول إلى النظام، فالكمبيوتر الشخصى يمكن إعطاء الحق لأكثر من شخص بالدخول عليه، وكذلك لبوابة المنزل أو غيرها، قد لا تحتاج للمفاتيح أو البطاقات فيما بعد فإصبعك يكفى للتزويد بتلك المعلومات أو نقلها، والشركات يمكنها تخزين معلومات تخص مئات الأشخاص، ولا تفتح الأبواب إلا إذا تطابقت البصمات الممسوح لها مع تلك المعلومات المخزنة.

استخدام البصمات البيومترية فى التحقق من هوية الأشخاص :

إن التطور التكنولوجى والتقنى الذى يعيشه العالم الآن جعل التحقق من هوية الأشخاص أمرًا يزداد صعوبة، ويرجع ذلك إلى تراجع الاتصال المباشر بين الأشخاص فى حياتهم اليومية بسبب الأجهزة والتقنيات التكنولوجية الحديثة فأغلب التعاملات تتم من خلال عمليات بسيطة على شبكة الإنترنت.

وقد استلزم هذا التطور الذى يشهده العصر واستفادت منه العناصر الإجرامية فى ارتكاب الجرائم، أهمية تطوير وتحديث الإجراءات الأمنية، ويعد استخدام البصمات البيومترية فى التحقق من هوية الأشخاص، إحدى الوسائل التى تعتمد عليها الأجهزة الأمنية فى كشف الجرائم ومرتكبيها.

أهم الوسائل البيومترية لتحقيق الهوية :

١ - بصمة الأصابع :

تكسو أصابع يد الإنسان خطوط حلمية بارزة توازيها أخرى غائرة، وتأخذ هذه الخطوط مسارات متعددة الاتجاهات، لتكون مجموعة من الأشكال الرئيسية والفرعية تتباين فيها العلامات المميزة لدرجة يصعب معها حصرها، وتبدأ تكوين هذه الأشكال بأطراف الجنين؛ حيث تكتمل سماتها المميزة فى الشهر السادس من الحمل، وتظل هذه الأشكال ثابتة لا يعتريها التغيير إلى ما بعد الوفاة، فهى آخر خلايا النسيج البشرى فى التحلل عدا ما يمكن أن يطرأ عليها من اتساع أو نعومة أو آثار لالتحام الجروح أو الحروق.

تتمثل وظيفة نظم التوثيق من خلال بصمات الأصابع التحقق من تطابق البصمات الرقمية للشخص المفحوص مع البصمات الرقمية التى تم تسجيلها مسبقًا للشخص نفسه فعند تسجيل البصمة يتم دعوة المستخدم لوضع إصبعه على جهاز القارئ، ثم يتم تحويل الصورة إلى بصمة رقمية يتم تحليلها للحصول على العلامات المميزة للبصمة، ثم يتم تخزينها على أقراص أو بطاقات، أما عند التحقيق من هوية شخص يتم دعوته إلى وضع إصبعه على جهاز القارئ، ثم تحول الصورة إلى صورة رقمية وتحلل لمعرفة العلامات المميزة، ثم تتم مقارنة البصمة المحولة مع البصمات التى سبق تسجيلها



للشخص نفسه، ومن خلال ذلك يسمح النظام ويرفض دخول الشخص وفقًا لنتيجة تتطابق بصمته مع البصمة التي سبق تسجيلها للشخص نفسه[1].

٢ - بصمة حدقة العين :

«الحدقة» هي الجزء الدائري الملون من العين، وهو الذي يتحكم في نسبة الضوء التي تدخل العين عن طريق فتح الحدقة وضمها بواسطة عضلة قابضة تتحكم في حجم حدقة العين فتسمح لمزيد من الضوء بالدخول للعين عندما يكون المكان مظلمًا وتسمح لكمية أقل من الضوء عندما يكون المكان مضاء.

وتستخدم في التصوير كاميرا متخصصة يقف أمامها الشخص، وترسم هذه الكاميرا خريطة واضحة للحدقة بدايةً من الحروف الخارجية للحدقة، ثم تنتقل تدريجيًا إلى المميزات الداخلية، وتسجيل البصمة لأول مرة يستغرق دقائق محدودة، والنظارات والعدسات اللاصقة لا تؤثر على المسح، ولا يتطلب توسع العين من جفونها لالتقاط الصورة أو التصاق مباشر بالكاميرا، أو تسليط ضوء في قاع العين كما هو حال بصمة شبكية العين، إلا أن تصوير الشخص بعدسة ذات حدقة مصطنعة يؤدي إلى خلل بالنظام.

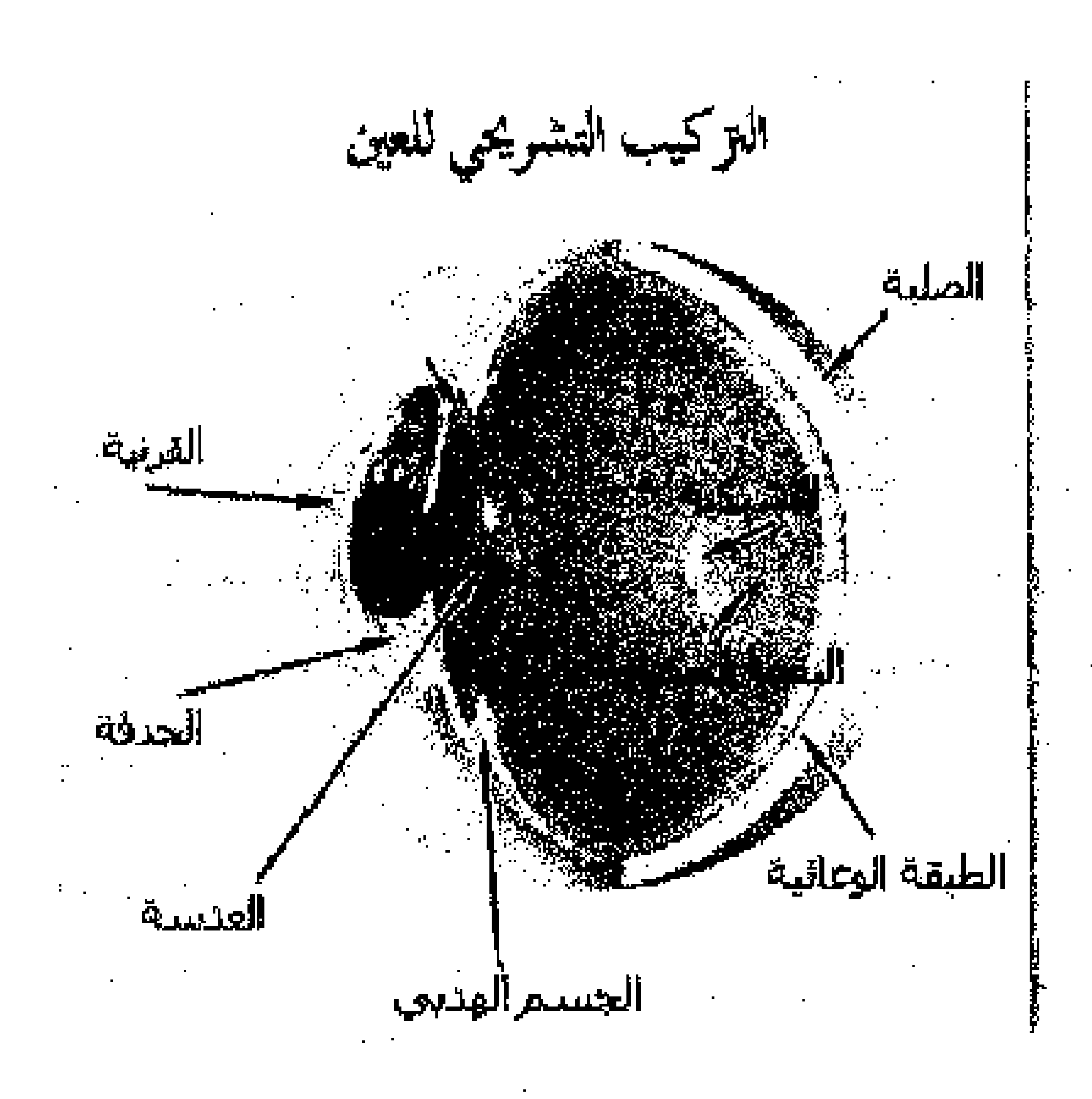
تحتوي حدقة العين على كم من المعلومات جعلها أكثر عضو مميز في جسم الإنسان على الإطلاق وجعل «البصمة الحدقية» أكثر تفوقًا في دقتها على كل الأنواع الأخرى ومن أجل التعرف على شخص، فالمسح الحدقي يتميز عن غيره من الوسائل بعدم وجود حدقتين متشابهتين في حدق البشر حتى في التوائم المتماثلة، بل إن الحدقة اليمنى ذاتها مختلفة عن اليسرى في الشخص الواحد، بالإضافة إلى أن رسم الحدقة ثابت

---

(1) Nalini Ratha, Ruud Bolle : Automatic Fingerprint Recognition Systems, New York: Springer, c2004, P52.

طوال العمر؛ حيث يتكون رسمه بعد ستة أشهر من الولادة ويثبت بعد سنة من العمر ويستمر في ثباته حتى الوفاة إلا في بعض العمليات الجراحية أو الحوادث النادرة، وعلى الشخص وقتها أن يعيد تسجيل بيانات حدقته.

المسح الحدقي هو الأكثر دقة وبساطة وخصوصية فيستحيل فيه أي نوع من التقليد، وأية مؤسسة تتعامل باستخدام المفاتيح، الكروت بأنواعها، الوثائق، الكلمات والأرقام السرية يمكن أن تستخدم هذا النوع من التكنولوجيا[1].



شكل رقم (١-٥) يوضح التركيب التشريحي للعين

(١) حسنين المحمدي بوادي: الوسائل العلمية الحديثة في الإثبات الجنائي، الإسكندرية، منشأة المعارف، ٢٠٠٥م، ص٦٤.



٣- بصمة راحة اليد :

إن استخدام الشكل الهندسي لليد هو الوسيلة الأكثر انتشارًا واستخدامًا للتحكم في المنافذ ويقوم النظام بالتحقق من (٩٠) علامة بما فيها البعد الثلاثي لليد وطول وعرض الأصابع وشكل المفاصل، والتقاط صورة لليد والحصول على معلومات عنها تستخدم الأشعة تحت الحمراء وكاميرا رقمية؛ حيث يضع المستخدم يده على لوح به علامات إرشادية لوضع الأصابع وتعطي أجهزة قراءة هندسة اليد مستوى عالٍ جدًا من الدقة إلا أنها يمكن أن تخطئ فيها بين التوائم أو أفراد العائلة الآخرين، كما أن هذه الأجهزة ذات حجم كبير مما يعوق استخدامها في بعض التطبيقات.

٤- بصمة سمات الوجه :

يتم استخدام قياسات خاصة بتباعد العينيين وحجم الأنف وعرض الفم للتعرف على هوية الأشخاص، وتستخدم معظم نظم التحقق من الوجه وسيلة نموذجية وهي جهاز الكمبيوتر وكاميرا لالتقاط الصورة وتسجيلها في قاعدة معلومات، وتستخدم تلك النظم قياسات تباعد بين مختلف أجزاء الوجه كوسيلة لتحقق من الشخص، إلا أن وجود متغيرات مثل النظارات الشمسية والذقن وتعبيرات الوجه غير العادية وانحناء الرأس يمكن أن تسبب خللاً بنظام تحديد الوجه[1].

٥- بصمة الصوت :

لكل صوت أيًا كان مصدرة مميزات وخواص معينة عن طريقها يمكن تمييزه عن مختلف الأصوات، وتتلخص هذه الخواص فيما يلي:

الدرجة : هي خاصية الصوت التي تجعلنا نميز بين نغمة غليظة ونغمة رقيقة.

(1) L.C. Jain : Intelligent Biometric Techniques in Fingerprint and Face Recognition, op.cit. p463

الشـدة : هي خاصية الصوت التي تجعلنا نميز بين نغمة قوية ونغمة ضعيفة.

النـوع: وهي خاصية الصوت التي تجعلنا نميز بين نوع المصدر الذي يصدر هذا الصوت أو هذه النغمة ويميز بين صوت بسيط وأصوات معقدة أو مركبة.

ويعتبر تحديد الصوت هو أحد الأشكال العادية جدًا في التكنولوجيا البيومترية لأنها لا تتطلب أي اتصال جسدي مع الجهاز القارئ بالنظام وتعتمد نظم تحديد الصوت على صفات الصوت الفريدة لكل شخص، وتستخدم أغلب نظم تحديد الصوت عرض نص ما وكلمات خاصة على الشخص قراءتها ونطقها من أجل التحقق من أن الشخص الجاري التحقق من هويته موجود ولا يتعلق الأمر بتسجيل له.

٦- بصمة شبكية العين :

هي الطبقة الحسية للعين ويخل فيها عدد كبير من الشعيرات الدموية التي يمكن أن يتغير شكلها من السن والمرض ولا يتغير شكلها الهندسي، فهي بصمة مميزة لكل شخص يمكن قياسها من خلال حزمة ضوئية يتم تسليطها على عين الشخص المراد التعرف عليه وتتميز تلك التقنية بأنها من أكثر الوسائل التي يمكن الوثوق بها في تحديد هوية التوائم المتماثلين ولكنها مكلفة للغاية.

وتلتقط الأجهزة القارئة حتى ١٩٢ نقطة أو علامة مميزة، يمكن استخدام هذا النوع من تحديد الهوية في تطبيقات أمان عالية للغاية.

٧- بصمة التوقيع :

إن التحقق (الحركي) من التوقيع يقوم على التفرقة بين أجزاء التوقيع المعتادة وأجزاء التوقيع التي تختلف مع كل توقيع، وتحتوي نظم التحقيق من الهوية من خلال التوقيع والمسح باستخدام قلم قارئ، ويتم التحقق من تحليل بعض المتغيرات منها سرعة التوقيع وزيادة سرعة التوقيع والضغط ... إلخ، ويتم ربط لوحة كتابة حساسة بجهاز



حاسب آلى يتم الكتابة عليه بقلم إلكتروني وفارة ويستخدم النظام برنامجًا خاصًا يعمل بالارتباط بقلم إلكترونى ويتم وفقًا لهذا النظام تسجيل حركات مستخدم القلم منها سرعة الكتابة، وتغيرات القلم وحساب المسافة ما بين الأحرف من خلال أخذ ثلاث عينات من التوقيعات يتم تحليلها وتسجيل التحليلات الناتجة فى قاعدة بيانات ويتم مضاهاة التوقيعات لمعرفة هوية الشخص[1].

ثانيًا- بصمة الإصبع:

البصمة هى حافة أصابع الأيدى، وأصابع القدمين، وكذلك راحة اليد، وراحة القدم، تحمل أثرًا طبيعيًا، عبارة عن صف من المسامات، متشكلة على شكل خرائط مناسيبة (Contour Map) ذات خطوط مناسيب أو كفاف (الشكل المنحرف أو المتعرج)، هذه الخطوط والمسامات تفرز عرقًا، والعرق يترك شكل مسامات على الأجسام الأخرى، خصوصًا الملساء، عند ملامستها لها، وهو ما يسمى «طبعة البصمة»، وتمتاز البصمات بخاصية تُعرف بالتفرد أو الفردية، إذ أن كل إنسان يحمل طبعة بصمة خاصة به، لم يثبت إلى الآن، تماثلها مع طبعة أو بصمة غيره.

وللبصمة صفات مميزة لكل شخص، فهى تتشكل عند الجنين حتى الأشهر السبعة الأولى من تكوينه، وتبقى مع الإنسان طيلة حياته، مع الإشارة إلى أن استخدام البصمة للتعرف على الهوية يعود إلى منتصف القرن التاسع عشر الميلادى، وشهد استخدامها تطورًا مهمًا فى نهاية القرن المذكور، كما أصبح استعمالها للتعرف على الهوية معتمدًا من الجهات القانونية، ويعود ذلك للمكانة المميزة التى تتبوؤها البصمة بين المحددات البيومترية المتنوعة المستخدمة للتأكد من الهوية[2].

---

(1) Nalini Ratha, Ruud Bolle, op.cit ,p45.

(2) Henry C. Lee, R.E. Gaensslen : Advances in Fingerprint Technology, 2nd ed, Boca Raton, Fla. : CRC Press, c2001, p 43.

لذلك فقد سعى العلماء لاكتشاف وسائل تجعل الكشف عن البصمات أكثر أمانًا، الطريقة البصرية المنتشرة بشكلٍ كبير تعتمد على صورة البصمة، فهى تقارن الشكل فقط، وهو ما دفع البعض للاتجاه إلى قياس مقاومة الجلد بالإضافة إلى الشكل، والطريقة الأكثر أمانًا هى الطريقة الحرارية؛ حيث تعتمد على قياس فرق درجة الحرارة بين المرتفعات والمنخفضات فى الإصبع أثناء ضغطه على الجهاز، وتعد هذه هى بصمة الإصبع التى تتم مقارنتها بالمعلومات المخزنة بقاعدة البيانات فى تلك التقنية الجديدة، هذه المعلومات الدقيقة تميز اليد، كما أن الإصبع يحمل فى المتوسط ٣٠ علامة دقيقة مميزة من سبعة أنواع مختلفة، وطريقة التخزين أيضًا مهمة جدًا؛ ولذلك فنحن نعتمد على العلامات الدقيقة فى الإصبع ونخزنها عن طريق الأعداد الثنائية (٠,١)، ومن غير الممكن حساب بصمة الإصبع عبر هذه الشفرة، ولكن بالتأكيد استخدام أكثر من ميزة بيومترية والجمع بينها هو ما يمكن أن يعطى أكبر قدر من الأمان لفتح الأبواب أو التعامل مع المعلومات.

واليوم يحلم العلماء بألا يقتصر الأمر على الأمان ولكنهم يحلمون أن تُستخدم التكنولوجيا كوسيلة للراحة أيضًا، فيحل الإصبع محل المفاتيح الكثيرة المتعبة التى يحملها الشخص فى كل مكان أو البطاقات التى تختلط بعضها ببعض والمعرضة لأن تفقد، وتعرض صاحبها للسرقة.

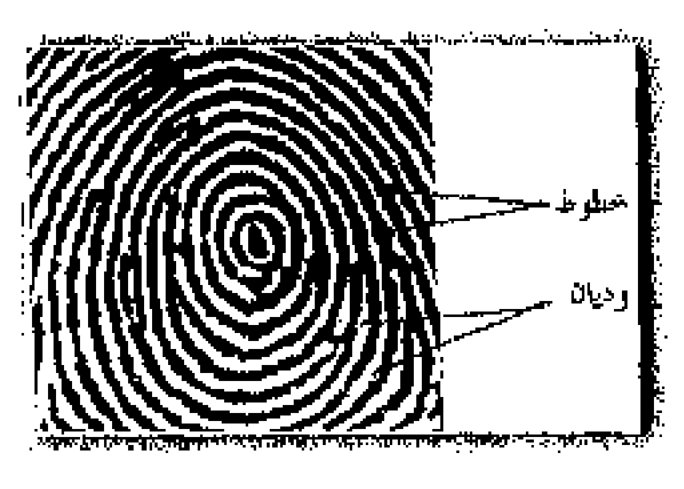
ويأمل العلماء أيضًا أن يكون الإصبع هو الوسيلة للدخول إلى المنزل أو محل العمل أو فتح بوابة جراج المنزل والمصعد وجهاز الكمبيوتر، هذا بالإضافة إلى توفير المزيد من الضمان عند سحب الأموال من ماكينات البنوك فى الشوارع.

وللبصمة شكل مميز لكل شخص، وهى تتكون قبل الولادة وتحتفظ بهذا الشكل المميز طوال فترة الحياة، وتتعرض للعديد من العوامل مثل السن، تأثير طبيعة العمل اليدوى،

الجروح، إلا أن الصفات المميزة لها تبقى موجودة، وتتمتع بمزايا تفضيلية مقارنة مع المحددات البيومترية الأخرى كسهولة الاستخدام، سرعة التصنيف، انخفاض كلفة التسجيل، إمكانية إيجاد البصمة في مكان الجرائم.

تصنيف البصمة :

البصمة عبارة عن شكل مؤلّف من مجموعة من الخطوط البارزة وفراغات بين هذه الخطوط تسمى بالأخاديد (أو الوديان)، وهى مجموعة من الخطوط والأخاديد والتى لها شكل مميز خاص بكل شخص تتم عملية التأكد من الهوية أو التعرف عليها[1].



شكل رقم (٢-٥) يوضح البصمة

وتصنيف البصمة هو عبارة عن تقنية تمكن من تحديد النوع الذي تنتمى إليه البصمة ضمن عدة أنواع محددة مسبقًا، مما يؤدي إلى مقارنة الدخل مع مجموعة فرعية من البصمات في قاعدة بيانات أنظمة التعرف على البصمة، والعمل على اختصار زمن البحث ودرجة تعقيد الحساب في هذه الأنظمة تشمل الأنواع الرئيسية لتصنيف البصمة خمس فئات وهى ما يلي:

(١) هويدا يسري عبد النبي سيد نافع : تطوير نظام آلي للتعرف على بصمة الإصبع، رسالة ماجستير ، جامعة حلوان ، الحاسبات والمعلومات، علوم الحاسب، القاهرة، ٢٠٠٥م.

أ- الحلقة اليسارية:

حيث يدخل خط واحد أو أكثر من خطوط البصمة من الجهة اليسارية، ثم يتقوس إلى الخلف ويخرج من الجهة نفسها التي دخل منها.



شكل رقم (٣-٥) يوضح الحلقة اليسارية

ب- الحلقة اليمينية:

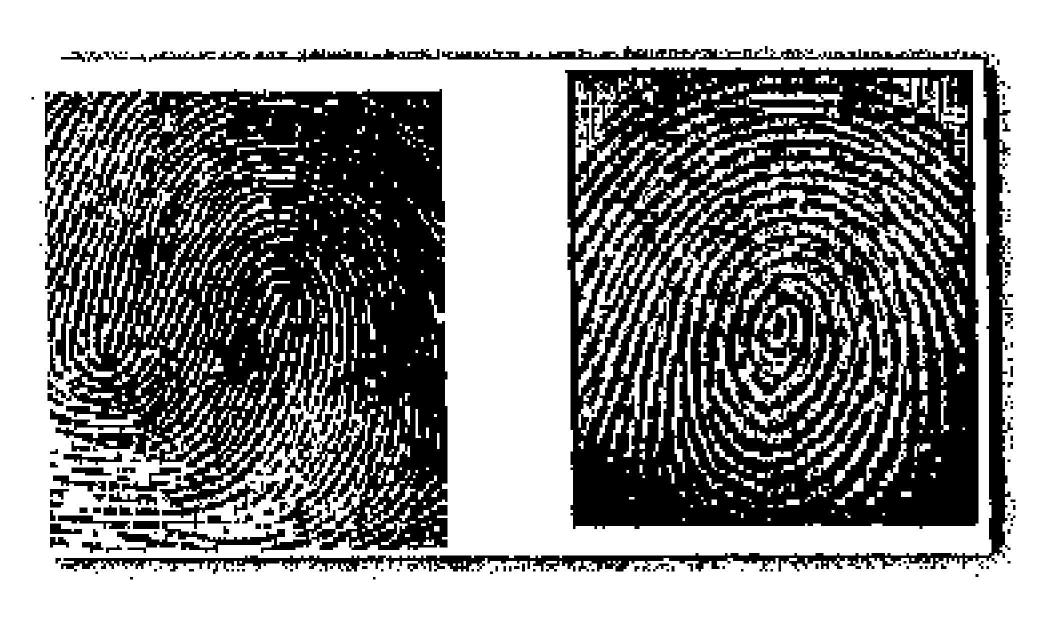
وهي مماثلة للحلقة اليسارية باستثناء كون خطوط البصمة تدخل وتخرج من الجهة اليمينية.



شكل رقم (٤-٥) يوضح الحلقة اليمينية

جـ- النوع الحلزوني:

حيث تحتوي البصمة على الأقل على خط واحد من خطوط البصمة والذي يشكل مسارًا كاملاً ٣٦٠ درجة (دائرة كاملة) حول مركز البصمة. ويمكن أن توجد فى هذا الصنف من البصمات حلقتان(أو حلزون واحد)، وهذا الصنف معقد جدًا، وأحيانًا يقسم إلى فئتين: الحلزون المنبسط والحلقة التوأم أو الحلقة المزدوجة.



شكل رقم (٥-٥) يوضح النموذج الحلزونى

د- القوس (القوس المنبسط):

حيث تدخل خطوط البصمة من جانب ما وتتجه إلى الجانب الآخر مع ارتفاع و تموج فى الوسط.



شكل رقم (٦-٥) يوضح القوس المنبسط

هـ- القوس على شكل خيمة:

وهو مماثل للنوع آنف الذكر، باستثناء وجود تقوس عالي لخط واحد من خطوط البصمة على الأقل.



شكل رقم (٧-٥) يوضح القوس على شكل خيمة

تصميم وتنفيذ النظام :

تتمحور النقاط الأساسية لتصميم نظام التعرف الآلي على البصمة حول اختيار طريقة عمل النظام («تأكد من الهوية» أو «تحديد الهوية»)، واختيار مكونات الكيانين الصلب واللين وجعلهما يعملان معًا. ويفضل طريقة «التأكد من البصمة» عندما يكون عدد المستخدمين كبيرًا، علمًا بأن النظام المعتمد على طريقة «تحديد الهوية» هو أكثر صعوبة في التصميم بسبب الوضع الحرج لمسألتي السرعة والدقة. وفي حال تصميم نظام يعتمد على بعض المكونات الجاهزة، فعلى مصمم النظام مراعاة مجموعة من العوامل عند انتقائه لهذه المكونات، مثل التقنية المستخدمة، ومدى توافق مواصفات هذه المكونات مع المتطلبات المحددة للمنتج النهائي، وتوافق البرمجيات مع منصة التشغيل، مع مراعاة التناقض بين الكلفة والأداء، وهو مرتبط بمتطلبات التطبيق، وتوفر الوثائق والدعم المناسبين من الجهات المنتجة لهذه المكونات.

ويتم التقاط صورة البصمة عن طريق الماسح الضوئى، ويتم إدخالها إلى وحدة التعرف؛ حيث تتم معالجة الإشارة الناجمة عن البصمة، ويتم استخلاص السمات الأساسية لها، وتحويلها إلى قيم رقمية خاصة بالبصمة المدخلة، وهنا يتم التمييز بين حالتين:

حالة التسجيل :

حيث تدخل البصمة إلى النظام لأول مرة وتقرن برقم شخصى خاص بمستخدم النظام ويتم إدخاله بواسطة لوحة الملامس، وفى هذه الحالة فإن سمات البصمة تخزن على شكل «قالب» فى قاعدة البيانات الموجودة ضمن وحدة التعرف، ويستخدم هذا القالب للمقارنة فى كل مرة يتم وضع البصمة ذاتها على الماسح وإدخال الرقم الشخصى المرتبط بها والمخزن فى قاعدة البيانات.

حالة استخدام النظام :

حيث يقوم المستخدم بإدخال البصمة المخزن قالبها وذلك بواسطة الماسح الضوئى، وإدخال رقمه الشخصي -أيضاً- بواسطة لوحة الملامس، وعندئذ تقوم وحدة التعرف باستخلاص السمات العائدة لهذه البصمة ومقارنتها مع القالب العائد للرقم الشخصى ذاته، وهنا يتم التمييز بين حالتين:

- حصول التطابق :

فى حالة حدوث تطابق فإن النظام يقبل المستخدم، سواءً كان فى حالة دخول أو خروج للمؤسسة، ويتم بيان ذلك بواسطة مؤشر ضوئى وتشكيل إشارة التحكم المناسبة، وإثبات توقيت العملية سواء كانت دخول أو خروج.

- عدم حصول التطابق :

وعندئذ فإن النظام لا يقبل المستخدم، ويتم بيان ذلك بواسطة مؤشر ضوئي أيضًا وإشعار مدير النظام بهذه النتيجة، وإخطاره بأن هناك محاولة دخول غير شرعية.

وفى كلتا الحالتين يتم تسجيل بيانات المستخدم فى قاعدة البيانات، وذلك لتوثيق هذه البيانات من جهة، ولإعداد التقارير المختلفة (اليومية، الأسبوعية، الشهرية) عن موظفى المؤسسة المستخدمة.

ثالثًا - البصمة الوراثية :

لم تُعرَف البصمة الوراثية حتى كان عام ١٩٨٤، حينما نَشر «د. آليك جيفريز» عالم الوراثة بجامعة «ليستر» بلندن بحثًا أوضح فيه أن المادة الوراثية قد تتكرر عدة مرات، وتعيد نفسها فى تتابعات عشوائية غير مفهومة، وواصل أبحاثه حتى توصل بعد عام واحد إلى أن هذه التتابعات مميِّزة لكل فرد، ولا يمكن أن تتشابه بين اثنين إلا فى حالات التوائم المتماثلة فقط؛ بل إن احتمال تشابه بصمتين وراثيتين بين شخص وآخر هو واحد فى التريليون، مما يجعل التشابه مستحيلاً؛ لأن سكان الأرض لا يتعدون المليارات الستة، وسجل الدكتور «آليك» براءة اكتشافه عام ١٩٨٥، وأطلق على هذه التتابعات اسم «البصمة الوراثية للإنسان «The DNA Fingerprint» ، وعرِّفت على أنها «وسيلة من وسائل التعرف على الشخص عن طريق مقارنة مقاطع (DNA)»، وتُسمَّى فى بعض الأحيان الطبعة الوراثية «DNA Typing»[1].

ولم تتوقف أبحاث «د.آليك» على هذه التقنية؛ بل قام بدراسة على إحدى العائلات يختبر فيها توريث هذه البصمة، وتبين له أن الأبناء يحملون خطوطًا يجيء نصفها من

(1) Henry C. Lee, R.E. Gaensslen : Advances in Fingerprint Technology, 2nd ed, Boca Raton, Fla. : CRC Press, c2001, p 34.



الأم، والنصف الآخر من الأب، وهى مع بساطتها تختلف من شخص لآخر. ويكفى لاختبار البصمة الوراثية نقطة دم صغيرة؛ بل إن شعرة واحدة إذا سقطت من جسم الشخص المُراد، أو لُعاب سال من فمه، أو أى شىء من لوازمه، فإن هذا كفيل بأن يوضح اختبار البصمة بوضوح.

وقد تمسح إذًا بصمة الأصابع بسهولة، ولكن بصمة الـ «(DNA)» يستحيل مسحها، وبمجرد المصافحة قد تنقل الـ «(DNA) الخاصة بالشخص إلى يد مَن يصافحه، والبصمة الوراثية لا تتغير من مكان لآخر فى جسم الإنسان، فهى ثابتة بغض النظر عن نوع النسيج، فالبصمة الوراثية التى فى العين تجد مثيلاتها فى الكبد، والقلب، والشعر.

تعريف البصمة الوراثية:

البصمة الوراثية عبارة عن عملية عزل للحمض النووي (DNA) عن مصادره الحيوية بواسطة إنزيمات خاصة تقسم هذا الحمض إلى مواقع قيد؛ حيث يكون له تسلسل معين، ومن ثَمَّ يتم تصنيف أجزاء الحمض النووى التي يتم الحصول عليها بهذه الطريقة بواسطة الأجهزة الكهربائية التى تتمثل فى أن يوضع المحلول الذى يحمل أجزاء الحمض النووى تحت مجال كهربائى، وبطريق خاصة يتم جعلها مرئية ويتم التمييز بين الأجزاء ووضع علامات على كل منها يمكن أن تظهر منه الركيزة (التصوير الإشعاعي الذاتى) وذلك يترك خطوط واضحة إلى حد ما والمقارنة من حيث العدد والمكان الخاص بصورتين إشعاعيتين يتيح الوصول إلى هوية مصدرها البيولوجى[1]، والحمض النووى عبارة عن مادة كيميائية تتحكم فى تطوير شكل الخلايا والأنسجة فى جسم الإنسان، فهو بمثابة خريطة خاصة بتطوير الجسم محفوظة فى داخل كل خلية من خلاياه.

---

(١) جميل عبد الباقى : أدلة الإثبات الجنائى والتكنولوجيا الحديثة، القاهرة، دار النهضة العربية للطبع والنشر والتوزيع، ٢٠٠٢م، ص٥٩.

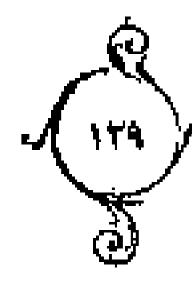
والحمض النووي يختصر بالأحـرف (DNA) وهـي الحروف الأولى لمصطلح (Deory Nevulice Acid) أي الحمض النووي وهي أيضًا عبارة عن مركب كيميائي معقد ذو وزن جزئي عالٍ لا يمكن للكائن الحي الاستغناء عنه يعرف (DNA) وهي اختصار لكلمة الحمض النووي الديوكسي منزوع الأكسجين والحمض النووي هو الذي يحمل المعلومات الوراثية ويكوّن من خطيين دائرين (النيوكليوتيدات) على شكل حلزون ويوجد هذا الحمض في أنوية الخلايا للكائنات الحية لذا يطلق عليه (الحمض النووي) وترجع أهمية الحمض النووي إلى أن الـ (DNA) في الخلية يشمل جميع الكروموسومات بداخل نواة الخلية وتشكل الكروموسومات نظامًا، وهذا النظام أو الترتيب هو الذي يحدد خصائص كل فرد باعتبار أنها تختلف من شخص لآخر.

التعريف الاصطلاحي للبصمة الوراثية :

اجتهد العلماء المعاصرون في وضع تعريف للبصمة الوراثية إلا أن تعريفاتهم تباينت، فهناك من عرفها بأنها «تعيين هوية الإنسان عن طريق تحليل جزء أو أجزاء من حمض (DNA) المتركز في نواة أية خلية من خلايا جسمه»، ورأى آخر يرى أنها «المادة الحاملة للعوامل الوراثية والجينات في الكائنات الحية»[1]، ورأى يرى أنها «صورة لتركيب المادة الحاملة للعوامل الوراثية أي هي صورة الحمض النووي (DNA) الذي يحتوي على الصفات الوراثية للإنسان أو بمعنى أدق هي صورة تابع النيوكليوثيدات التي تكون جزء الحمض النووي الوراثي DNA، وتعد وسيلة من وسائل التعرف على الشخص عن طريق مقارنة مقاطع الـ (DNA)».

ونميل إلى الرأي الذي يرى أن البصمة الوراثية هي «تعيين هوية الإنسان عن طريق تحليل جزء أو أجزاء من الحمض النووي المتمركز في نواة أية خلية من خلايا جسمه؛

(١) طارق إبراهيم الدسوقي عطية : البصمات وأثرها في الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، ٢٠١١م، ص٥١.



حيث إن تلك المادة حاملة للعوامل الوراثية والجينات فى الكائنات الحية بالنواة».

مجالات العمل بالبصمة الوراثية :

يرى المختصون وخبراء البصمات أنه يمكن استخدام البصمات الوراثية فى مجالات كثيرة، ترجع فى مجملها إلى مجالين رئيسيين، هما:

١ - المجال الجنائى:

وهو مجال واسع يدخل ضمنه الكشف عن هوية المجرمين فى حالة ارتكاب جناية قتل، أو اعتداء، وفى حالات الاختطاف بأنواعها، وفى حالة انتحال شخصيات الآخرين ونحو هذه المجالات الجنائية[1].

٢- مجال النسب :

وذلك فى حالة الحاجة إلى إثبات البنوة أو الأبوة لشخص، أو نفيه عنه، وفى حالة اتهام المرأة بالحمل من وطء شبهة، أو زنا.

خصائص البصمة الوراثية:

١- تتمتع البصمة الوراثية بميزة الدقة، وتعتبر أدق وسيلة عُرفت حتى الآن فى تحديد هوية الإنسان، وذلك لأن نتائجها قطعية لا تقبل الشك، وإحدى المشاكل التي لم تجد حلاً فى الطرق التقليدية هى فحص المادة الجسدية المختلطة مثل الحيوانات المنوية المخلوطة بالإفرازات المهبلية، أما بالنسبة لاختبار الحمض النووى فلا يُشكل مثل هذا الاختلاط أية مشكلة فى الكشف عن تركيب هذا الحمض، ولذلك أهميته فى قضايا القتل الجنسي بصفة خاصة بحيث تختلط الحيوانات المنوية للجانى بالإفرازات المهبلية للمجنى عليها.

(١) محمد أحمد غانم : الجوانب القانونية والشرعية للإثبات الجنائي بالشفرة الوراثية، القاهرة ، بدون ناشر، ص٦٠.

٢- يعتبر تحليل الـ (DNA) (البصمة الوراثية)، وسيلة فعَّالة فى مجال البحث عن الحقيقة من حيث إثبات الجريمة أو نفيها بدقة تامة؛ حيث توجد فى كل خلية فى جسم الإنسان بطاقة لا يمكن تزويرها فيمكن مقارنة منطقة الحمض النووى الذى يعتمد عليه فى مكان وقوع الجريمة بمنطقة الحمض النووى للمادة أو الخلية المأخوذة من المتهم، ووجود منطقتين متطابقتين يعتبر دليلاً شبه مطلق على أن الخلية هى للشخص نفسه، فيما عدا حالة وجود توأم آحادى البويضة حيث لا يمكن الجزم بذلك.

٣- البصمة الوراثية التى يحملها الحمض النووى شديدة المقاومة ولا تتأثر بالظروف الجوية من حرارة، ورطوبة، وجفاف، ولا تتلف وتقاوم عوامل التحلل والتعفن، ويمكن حفظها واستخدامها لعدة سنوات فيمكن عمل البصمة من الآثار الحديثة والقديمة جدًا.

٤- أن تركيب جزئى الحمض النووى لا يختلف من خلية لأخرى، فالحمض النووى فى أية خلية دموية يطابق تمامًا الحمض الموجود فى أية مادة حيوية، بمعنى أن الحمض النووى لدى الأفراد متطابق فى كل خلايا الجسم ولا يتغير أثناء الحياة[1].

٥- عدم إمكانية الخلط بين جزئين متواجدين فى مسرح الجريمة ولكن لشخصين مختلفين؛ حيث يمكن الفصل بينهما مهما كان الحال من الاختلاط، فيسهل فيها الفرز.

٦- للبصمة الوراثية الميزة الفنية التي تقطع الشك باليقين، تعتبر دليل نفى وإثبات قاطع بنسبة ١٠٠ ٪ ، وذلك لأن احتمال التشابه بين البشر فى الـ (DNA) غير

(١) رمسيس بهنام ، البوليس العلمي وفن التحقيق، منشأة المعارف بالإسكندرية ١٩٩٦م، ص٧٠.



وارد، بعكس فصائل الدم، التى تعتبر وسيلة نفى فقط لاحتمال التشابه بين البشر فى هذه الفصائل.

٧- يمكن التوصل للبصمة الوراثية لأى شخص بالبحث والفحص الدقيق للحمض النووى، من أية مخلفات آدمية سائلة (دم، منى، لُعاب) أو أنسجة (لحم ،عظم، شعر) وهذه ميزة مهمة فى حالة عدم العثور على بصمات أصابع المجرم.

٨- البصمة الوراثية (DNA) توجد فى أنوية جميع الخلايا باستثناء كرات الدم الحمراء؛ حيث لا يوجد فيها نواة، ولذلك يمكن استخراج سائل النواة الـ (DNA) بسهولة من جذور الشعر وكرات الدم البيضاء والعظام وإفرازات الإنسان كالمني واللُعاب والفضلات، وبذلك يمكن مقارنة المادة الحيوية لإحدى الخلايا مثل الخلية الدموية، بمادة أخرى مثل الغشاء المخاطي لغدة الفم، وقد أثبتت التجارب والاختبارات أن لكل مخلوق (DNA) متفرد فى الشكل والطول والمميزات ومواقع الترسيب ما عدا التوأم الذى يأتى من بويضة واحدة.

٩- على أثر نجاح البصمة الوراثية وما تتمتع به من خصائص ومميزات، والمكانة التى تستعدى أن يستعان بها الخبراء، وإمكانية تحديد هوية الأشخاص، كما أنها من أدق الوسائل للتوصل إلى الفاعل الحقيقى بأسرع الطرق ، وذلك اعتمد مكتب التحقيقات الفيدرالية بالولايات المتحدة الأمريكية طريقة اختبار سائل نواة الخلية (DNA) كإحدى الوسائل المعتمدة فى إجراءات البحث الجنائى.

١٠- تظهر بصمة الحمض النووى على هيئة خطوط عرضية يسهل قراءتها وحفظها وتخزينها فى الكومبيوتر لحين الطلب للمقارنة، بعكس بصمات الأصابع، التى لا يمكن حفظها فى الكومبيوتر، شرعت بعض الدول بتأسيس بنك لقاعدة بيانات الحمض النووى لكافة مواطنيها، ودول أخرى اقتصرت على المشتبه

فيهم، كى يكون لديها دليل فى حالة الاشتباه وفى حالة الاختفاء.

١١- أهم مميزات البصمة الوراثية فى تفرد كل شخص بها على حده دون خلط مما يساعد على جلاء الحق وإزالة أية شوائب تشويه، بل والتثبت على اليقين دون الشك وذلك فيما عدا حالة التوائم المتشابهة، ويمكن الحصول عليها من أى من أجزاء الجسم حتى فى حالة التعفن.



قائمة المراجع

قائمة المراجع

أولاً-الكتب :

أحمد سيد مصطفى : **إدارة الإنتاج والعمليات فى الصناعة والخدمات**، مكتبة الأنجلو المصرية، الطبعة الثالثة، القاهرة، ١٩٩٧م .

- المدير العربى فى عالم متغير، القاهرة، بدون ناشر، القاهرة،٢٠٠٢م.

إسماعيل محمد السيد : **نظم المعلومات لاتخاذ القرارات الإدارية**، الإسكندرية، المكتب العربى الحديث للطباعة والنشر، ٢٠٠١م.

أشرف السعيد أحمد : **تكنولوجيا المعلومات وإدارة الأزمات**، القاهرة، ٢٠١٣م.

- **أثر تكنولوجيا الأزمات على إدارة الأزمة الأمنية** (دراسة تطبيقية)، القاهرة، ٢٠١١م.
- **القرصنة الإلكترونية**، القاهرة، ٢٠١٢م.
- **مقدمة فى علوم الحاسب**، القاهرة ،٢٠١١م.

جميل عبد الباقى : **أدلة الإثبات الجنائى والتكنولوجيا الحديثة**، القاهرة، دار النهضة العربية ، ٢٠٠٢م.

حسن على الزغبى : **نظم المعلومات الاستراتيجية**، عمان، دار وائل للنشر والتوزيع، الطبعة الأولى، ٢٠٠٥م.

حسن عماد مكاوى : **تكنولوجيا الاتصال الحديثة فى عصر المعلومات**، الطبعة الأولى، القاهرة، الدار المصرية اللبنانية، ١٩٩٣م.

حسنين المحمدى بوادى : **الوسائل العلمية الحديثة فى الإثبات الجنائى**، الإسكندرية ،منشأه المعارف، ٢٠٠٥م.

خالد ممدوح إبراهيم : **أمن الحكومة الإلكترونية**، الإسكندرية، الدار الجامعية، ٢٠٠٨م.

رأفت رضوان : **الحكومة الإلكترونية**، القاهرة، المركز الدولى للدراسات المستقبلية و الإستراتيجية، ٢٠٠٥م.

رمسيس بهنام : **البوليس العلمي وفن التحقيق**، منشأة المعارف بالإسكندرية ١٩٩٦م.

طارق إبراهيم الدسوقى : **البصمات وأثرها فى الإثبات الجنائي**، دار الجامعة الجديدة، الإسكندرية، ٢٠١١م.

- **الأمن المعلوماتى**، النظام القانونى لحماية المعلومات، القاهرة، دار الجامعة الجديدة،٢٠٠٩م.

طارق طه : **نظم المعلومات والحاسبات الآلية من منظور إدارى**، القاهرة، دار الفكر العربى، ٢٠٠٨م.

عبد الحكم أحمد الخزامى : **فن اتخاذ القرار مدخل تطبيقى**، مكتبة ابن سينا ، القاهرة، ١٩٩٩م.

عصمت عبد الله الشيخ : **دور نظم وتكنولوجيا المعلومات فى تيسير وفاعلية العمل الإدارى**، دار النهضة العربية، ١٩٩٨م.

علاء عبد الرازق السالمى : **نظم إدارة المعلومات**، الدوحة - قطر، المنظمة العربية للتنمية الإدارية، ٢٠٠٢م.

على عبد الهادى مسلم : **مذكرات فى نظم المعلومات المبنية على الكمبيوتر- المبادئ والتطبيقات**، مركز التنمية الإدارية، جامعة الإسكندرية، ١٩٩٤م.

علـــى فـهـمـــى : **نظم دعم اتخاذ القرار والأنظمة الذكية**، القاهرة، دار الكتب للنشر والتوزيع، القاهرة، ٢٠٠٤م.

عماد عبد الوهاب الصباغ : **علم المعلومات**، دار الثقافة للنشر والتوزيع ، قطر، ٢٠٠٤م.

فـريـد الـنـجـار : **الحكومة الإلكترونية**، بين النظرية والتطبيق، الإسكندرية، الدار الجامعية، ٢٠٠٨م.

محمد أحمد غانم : **الجوانب القانونية والشرعية للإثبات الجنائى بالشفرة الوراثية**، القاهرة ، ٢٠٠٧م.

محمد السعيد خشبة : **نظم المعلومات المفاهيم والتكنولوجيا**، دار الإشعاع للطباعة، القاهرة، ١٩٨٧م.

محمد محمد الهادى : **التطورات الحديثة لنظم المعلومات المبنية على الكمبيوتر**، القاهرة، دار الشروق، ١٩٩٣م.

ثانيًا - الأبحاث والدراسات:

أحمد سيد مصطفى : انعكاسات التكنولوجيا على العنصر البشري في المنظمات العربية، ورقة عمل نشرت بمجلة آفاق اقتصادية، العدد ٧٣، مجلد١٩، ١٩٨٩م.

هويدا يسري عبدالنبي سيد نافع: **تطوير نظام آلي للتعرف على بصمة الأصبع**، رسالة ماجستير، جامعة حلوان، الحاسبات والمعلومات، علوم الحاسب، القاهرة،٢٠٠٩م.

يونس عرب : **الخصوصية وأمن المعلومات**، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي – اتحاد المصارف العربية ، ٢٠ – ٢٢ أيار ٢٠٠١ ، عمان - الأردن، ٢٠٠١م

ثالثًا - الندوات:

ندوة تكنولوجيا المعلومات الأمنية، سنوات من التحديث والإنجاز، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠٠٤م.

رابعًا - الكتب والمراجع الأجنبية:

Bhunia, C.T : **Information Technology Network**, New AGE, 2005

Collin, S. M. H : **Dictionary of Information Technology**, London: Peter Collin Pub, 1996.

E.Wainright Martin : **Managing Information Technology : What Managers Need To Know?** (New Jersey : Prentice Hall), 1999.

Fletcher, Keith : **Marketing Management And Information Technology,** New York: Prentice Hall, 1995.

Gershenfeld, Neil : **The Physics Of Information Technology** ,Cambridge; New York : Cambridge University Press ,2000.

Henry C. Lee, R.E : **Gaensslen, Advances in Fingerprint Technology,** 2nd ed, Boca Raton, Fla. : CRC Press, c2001.

Henry C. Lee, R.E Gaensslen. : **Advances in Fingerprint Technology,** 2nd ed, Boca Raton, Fla. : CRC Press, c2001.

Horrington Jon : **Organization Structure And Information Technology,** New York Prentice Hall International , 1991.

Indira Carr : **Computer Crime International Library of Criminolgy,** Criminal Justice and Penology - Second Series Ashgate, C2009.

K. Samuelson and H. Borko and G.X.Aney. : **Information System And Network Amsterdan :** North Holand Publishing Co.,)1977.

Karl De Leeuw, J. A. Bergstra. : **The History of Information Security:** A Comprehensive Handbook, Elsevier, 2007.

Kimberly Kiefer : **Information Security:** A Legal, Business, and Technical Handbook, American Bar Association, C2004

L. Jean Camp, Stephen Lewis. : **Economics of Information Security,** Springer, C2004.

L.C. Jain : **Intelligent biometric techniques in fingerprint and face recognition**, Boca Raton: CRC Press, C1999

Lucas, Henry C : **Information Technology For Management** -7 th ed (Boston :Irwin /McGraw -Hill), 2000.

Nalini Ratha, Ruud Bolle. : **Automatic Fingerprint Recognition Systems**, New York: Springer, c2004.

O'Brien ,James A : **Management Information Systems** :3rd ed ,Chicago: Irwin, 1996.

ohn R. Vacca : **Computer and Information Security Handbook**, Morgan Kaufmann, C2009.

Oliver. E.C. : Chapman, R.J. French, C.S. : **Data processing And Information Technology** -8 ed, DP Publications, Reviser, 1990.

Owen, Jo : **The leadership skills handbook**, London; Philadelphia: Kogan Page,2006.

Paulus R. Wayleith : **Data Security: Laws and Safeguards**, Nova Science Publishers, C2008.

Rosenthal, Uriel, Pijnenburg, Bert. : **Crisis Management and Decision Making**, Dordrecht, Boston :Kluwer Academic Publishers,1991.

Tyler Moore : **Economics of Information Security and Privacy**, Springer, C2010.

Weisman, H.M : **Information Systems Services And Centers.** London: John Wiley، 1972.

Williams, Brian K, Sawyer, Stacey C. : **Using Information Technology**, 4 th ed,Boston: McGraw - Hill,2001.

Yadav,D.S : **Foundations Of Information Technology**-3 rd ed, New age international limted publishers ,2006.

خامسًا - مواقع الإنترنت:

- www.egypt.gov.eg



فهرس الموضوعات

الفهـــرس

الموضـــــوع | الصفحة

الموضـــــوع	الصفحة

دار الكتاب الحديث :

- العنوان : ٩٤ش عباس العقاد - مدينة نصر - القاهرة

- تليفون : ٢٢٧٥٢٩٩٥ - ٢٢٧٥٢٩٩٣

المجموعة العربية للاستشارات والتدريب والنشر:

- العنوان : ٨أ ش أحمد فخري - مدينة نصر - القاهرة

- تليفون : ٢٢٧٣٩١١٠

دار العلوم للنشر والتوزيع :

- العنوان : ٢٩ش ٩ - ثكنات المعادى - القاهرة

- تليفون : ٢٣٥٩٣٩١٨

دار الفكر العربي :

- العنوان : ٩٤ شارع عباس العقاد - مدينة نصر - القاهرة

- تليفون : ٢٢٧٥٢٩٨٤

- العنوان : ١٦أ شارع جواد حسنى - القاهرة

- تليفون : ٢٣٩٣٠١٦٧

دار النهضة العربية :

- العنوان : ٣٢ ش عبدالخالق ثروت - القاهرة

- تليفون : ٢٣٩٢٦٩٣١



للكميات : ASHRAF.M3R62@GMAIL.COM

Inv:2975

Date:20/4/2014



تكنولوجيا المعلومات
فى المجال الأمنى

يتناول هذا الكتاب دور المعلومات فى نتاج البشر، حيث أصبح يقاس التقدم فى أية مهنة أو منظمة أو دولة بما يتوافر لدى أى منهم من مستودع من المعلومات، ولقد أثر التطور السريع لتكنولوجيا المعلومات تأثيرًا كبيرًا وبالغًا فى واقع العمل الأمنى، وكان لوزارة الداخلية الحرص على مواكبة التقدم التكنولوجى وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية فى مصر، بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية الحديثة، وقد تناولنا الموضوع من خلال خمسة فصول: الفصل الأول بعنوان تكنولوجيا المعلومات، ونعرض من خلاله ماهية التكنولوجيا وخصائصها، ومفهوم وأنواع نظم المعلومات، والفصل الثانى بعنوان تكنولوجيا المعلومات الأمنية، وتناولنا من خلاله نشأة نظام المعلومات، والتخطيط الاستراتيجى لتطوير نظم المعلومات بوزارة الداخلية، وأهداف وخصائص تكنولوجيا المعلومات الأمنية، ومدى الحاجة لتكنولوجيا المعلومات فى العمل الأمنى، والفصل الثالث بعنوان استراتيجية أمن المعلومات، وتناولنا من خلاله مفهوم أمن المعلومات، ومفهوم الاستراتيجية، وأهم أساليب تأمين قواعد البيانات، والفصل الرابع بعنوان تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية، وتناولنا من خلاله مفهوم الحكومة الإلكترونية، وتطبيقات وزارة الداخلية المصرية فى مجال الحكومة الإلكترونية، والفصل الخامس بعنوان دور التقنيات الحديثة فى تطوير تكنولوجيا المعلومات الأمنية، مفهوم التقنية البيومترية، وبصمة الإصبع، البصمة الوراثية. وندعو الله أن نكون قد وفقنا فى المساهمة ولو بشكلٍ بسيط فى عرض المعلومات الأساسية، التى تساعد الباحثين والمهتمين بمجال تكنولوجيا المعلومات الأمنية لمواكبة عصر تكنولوجيا المعلومات.



من الإصدارات السابقة

يُطلب من المكتبات التالية :
دار الفكر العربى - دار العلوم للنشر والتوزيع - دار النهضة العربية
دار الكتاب الحديث - المجموعة العربية للاستشارات والتدريب والنشر

مطابع الشرطة: ٢٠٢٠-٢٥٩٠